Authentication and Security

Product Summary

March 11, 2025

Contents

Authentication and Security

In this book, you can learn about Workday authentication and security features.

Authentication

Authentication Policies

Steps: Set Up Authentication Policies

Prerequisites

- Review Concept: Authentication Policy Best Practices on page 16.
- Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can create authentication policies that determine how users can access your Workday tenant. When defining an authentication policy, consider:

- Workday environments for which you're creating the authentication policy.
- Networks and IP addresses from which you want to block all users.
- Networks and IP addresses for which you want to enable access to users.
- Methods you want to require users to authenticate with, and if you want to require multifactor authentication for users.
- Functionality to which you want to restrict users after they authenticate.

Steps

1. Access the **Manage Authentication Policies** report to create or edit an authentication policy.
2. From the **Restricted to Environment** prompt, select 1 or more environments to apply the authentication policy to.

   For an authentication policy to apply, the current environment must match an environment set for the authentication policy. If it does, then Workday evaluates the list of rules for the first rule that applies to the user. If it doesn't, Workday proceeds to the next authentication policy.

   Note: To apply the authentication policy to your Sandbox Preview or Implementation Preview tenant, select *Sandbox* or *Implementation* respectively at the **Restricted to Environment** prompt. Those environments also apply to the respective tenants.
3. (Optional) Select the **Authentication Policy Enabled** check box to enable the authentication policy for the selected environments.

   You can enable only 1 authentication policy per environment.

4. (Optional) From the **Network Denylist** prompt, select networks for which you want to block users from accessing Workday. You can click **Manage Networks** to define IP ranges.

   Workday extends IP restrictions imposed by the denied IP ranges throughout the sessions of your users. If a user signs in from an IP address that Workday doesn't deny, but then switches to an address that Workday denies, Workday:

   - Terminates the user session.
   - Posts an authentication failure message in the **Signons and Attempted Signons** report. The message states that Workday doesn't allow the originating IP address based on the IP restrictions set for the system account. The message also includes the IP address.

   See Maintain IP Ranges on page 11.
5. (Optional) Add Authentication Rules on page 8.

   Under **Authentication Allowlist**, define networks and authentication types that selected security groups can use to access Workday. You can also set access restrictions that limit access after sign-in.
6. (Optional) Configure step up authentication.

   See Steps: Configure Step Up Authentication on page 35.
7. Activate Pending Authentication Policy Changes on page 15.

Result

When processing an applicable authentication policy, Workday evaluates:

1. Blocked networks.
2. Authentication rules in order.

Workday applies the first rule that matches the user based on security group membership.

Next Steps

Access the **Signons and Attempted Signons** report to review sign-in errors related to authentication policies.

Related Information

Concepts

Concept: Authentication Policies on page 18
Concept: Authentication Policy Best Practices on page 16

Add Authentication Rules

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can define authentication rules as part of the setup process for authentication policies.

Workday uses authentication rules to determine sign-in conditions for different groups of users. Groups of users are determined by the security groups to which the users belong. Your authentication policy can consist of many authentication rules.

Each authentication rule can consist of 1 or more authentication conditions. You can create multiple authentication conditions to define sign-in conditions within a group of users. Example: Users signing in over a defined network can have sign-in conditions that are different from users in the same user group who sign in from outside that network.

Steps

1. Access the **Manage Authentication Policies** report and edit the authentication policy to which you want to add your authentication rules.
2. Click a plus (+) icon in the leftmost column of the **Authentication Ruleset** grid to add a new blank authentication rule.

   A new authentication rule automatically contains 1 blank authentication condition.
3. Enter a name for the rule in the **Authentication Rule Name** field.
4. In the **Security Group** field for the rule, select the unconstrained security groups to which you want the rule to apply.
5. Enter a name for the authentication condition in the **Authentication Condition Name** field.

   The fields in the remaining columns are relevant to this authentication condition.
6. In the **Authentication Conditions** column, select a condition under which members of the selected security groups can access Workday:

   - **Specific**, and create or select specific networks or IP ranges from which security group members can access Workday.
   - **Any** or **Any except other conditions**, to enable security group members to access Workday from any network. These 2 selections have further dependencies on selections that you make in other authentication conditions you create for the rule. See **How Workday Processes Authentication Policies** in Concept: Authentication Policies on page 18 for more information.

   Workday extends IP restrictions imposed by specific IP ranges throughout user sessions. If a user signs in from an IP address in an allowed network but then switches to an address that's not in the allowed networks, Workday:

   - Terminates the user session.
   - Posts an authentication failure message in the **Signons and Attempted Signons** report. The message states that Workday doesn't allow the originating IP address based on the IP restrictions set for the system account. The message also includes the IP address.

   Note: Workday doesn't apply IP range restrictions to requests originating from our integration system when those requests come from Workday Internal IP addresses. If an integration system request includes an external IP address, Workday applies the appropriate authentication rule.
7. (Optional) Select **Device is Managed** to specify that the group of users can access Workday only when signing in from a managed device.

   A managed device is a device that a third-party mobile device management (MDM) provider administers for your organization. You can use **Device is Managed** on an authentication condition only if:

   - You've selected Security Assertion Markup Language (SAML) as an authentication type.
   - You've specified a **Managed Device Attribute** on the **Edit Tenant Setup - Security** task for the SAML IdP used for authentication.
8. In the **Allowed Authentication Types** column, select the type of authentication allowed for the users meeting the configured authentication condition.

   Workday automatically selects **Any**, which means that users meeting the authentication condition can sign in to Workday using any available authentication type. To restrict access, select **None** to block access using all available authentication types, or select **Specific** and configure at least 1 authentication type.
9. As you configure a **Specific** authentication type, consider:

Option	Description
Mobile PIN/Biometric	Enables the specified security groups to sign in using the Workday mobile apps. This authentication type requires a second enabled authentication type so that users can sign in to

Option	Description
	Workday to set up biometric authentication or their PIN.
OpenID Connect	Workday recommends that you select **Multi-factor Authentication** providers for this authentication type.
SAML	Enables access using any SAML IdP configured for the same environment as the authentication policy. Workday recommends that you select **Multi-factor Authentication** providers for this authentication type. To select **Multi-factor Authentication** providers, you must first select **Enable Native Multi-Factor Authentication** on the **Edit Tenant Setup - Security** task. If the applicable rule uses SAML, the current environment must also match the environment for the SAML IdP, as defined on the **Edit Tenant Setup - Security** task.
SAML: <IdP name>	Select 1 or more SAML IdPs for the rule. Workday automatically populates this list with the SAML IdPs defined on the **Edit Tenant Setup - Security** task for the same environment as the authentication policy. Workday recommends that you select **Multi-factor Authentication** providers for this authentication type. To select **Multi-factor Authentication** providers, you must first select **Enable Native Multi-Factor Authentication** on the **Edit Tenant Setup - Security** task.
User Name Password	Workday recommends that you select **Multi-factor Authentication** providers for this authentication type.
User Name Password + Challenge Questions (Do Not Use)	If you've enabled delegated authentication for your tenant or for particular users, you can select this option. Workday doesn't require web services users to answer challenge questions. **Note:** Workday plans to retire challenge questions in a future release. We recommend that you use other forms of authentication that we support.
WebAuthn (FIDO2)	To select this authentication type, you must enable web authentication on the **Edit Tenant Setup – Security** task. Also specify 1 of these authentication types on the rule: • **User Name Password** • **User Name Password + Challenge Questions (Do Not Use)**

Option	Description
	You can also specify **Mobile PIN/Biometric** as an allowed authentication type on the rule.
X509	Recommended for web services users and integrations that use an integration system user account.

10. (Optional) Select or create an **Access Restriction for Authentication Condition**.

    Access restrictions limit the access of the security groups to certain functionality based on how they sign in to Workday. See Create Access Restrictions.

11. (Optional) Create any other authentication conditions that you want to include on the authentication rule.

    Click a plus (+) icon in the column to the right of the **Security Group** column to add authentication conditions on the rule.

12. Once you've completed adding authentication conditions on the rule, **Order** them in the sequence that you want Workday to evaluate them within the rule.

Next Steps

Activate Pending Authentication Policy Changes on page 15

Related Information

Tasks

Create Access Restrictions on page 12
Set Up Workday Web Service Authentication on page 229

Reference

Reference: Edit Tenant Setup - Security

Maintain IP Ranges

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can define ranges of IP addresses as client networks and use them in authentication policies to designate blocked and allowed networks for accessing Workday.

Steps

1. Access the **Maintain IP Ranges** task.

2. Add a row to define a network, and in the **IP Range** box, enter a comma-separated list of IP addresses using one of these formats:
   - X.X.X.X
   - CIDR notation. Example: 192.168.0.1/24
   - X.X.X.X - Y.Y.Y.Y

   Note: Workday has a limitation on IP ranges that include a dash. If you experience sign-in errors in the **Signons and Attempted Signons** report after you begin using an IP range that is in that format:

   a. Use a tool that converts IP address ranges to CIDR notation, and see if the range breaks down to a series of smaller segments. Such third-party CIDR calculator tools are available online.
   b. Reenter the **IP Range** in Workday as a comma-separated list of the segments returned by the tool. Example: 199.67.128.0/18, 199.67.192.0/24 or 199.67.128.0-199.67.191.255, 199.67.192.0-199.67.192.255.
3. (Optional) Select the **Inactive** check box to deactivate an IP range.

   Inactive IP ranges aren't selectable for use in authentication policies. Clear the **Inactive** check box for a given IP range before you can select it for use in an authentication policy.
4. Access the **Activate All Pending Authentication Policy Changes** task to confirm changes.

Result

You can select the network when setting up a **Network Denylist** or specifying allowed networks (under **Authentication Condition**) for an authentication rule on an authentication policy.

Next Steps

Access the **View IP Range** report or these tasks to manage IP ranges:

- **Create IP Range**
- **Edit IP Range**
- **Delete IP Range**

Note: To delete a given IP range, deactivate it first. You can't deactivate an IP range that you include in an authentication policy, whether or not that authentication policy is active.

Create Access Restrictions

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can:

- Limit the access of users to Workday functionality based on how they sign in to their Workday session.
- Create an access restriction and apply it as a condition on an authentication rule in an authentication policy.
- Configure different access levels and authentication for users working outside the corporate network.

Steps

1. On a condition for an authentication policy rule, access the **Create Access Restriction** task. You can access the task from the **Access Restriction for Authentication Condition** column of the **Authentication Ruleset** grid for the condition.

2. From the **Allows Access to Security Groups** prompt, select the security groups to which you want to enable access. If you don't select any security groups, you're authorizing access to all security groups.

   When you want to select these types of context-sensitive security groups, also select the component security groups within the context-sensitive security groups:

   - Aggregation
   - Intersection
   - Segment-based

   Example: You want to add a segment-based security group named Worker Access to All Topics to the access restriction, and that security group contains these security groups:

   - All Contingent Workers
   - All Employees
   - All Pre-Employees

   Add all 4 security groups to **Allows Access to Security Groups**.

   When you select a context-sensitive security group, users might have more access than you want to grant, as users will have access to:

   - All items secured by the context-sensitive security group.
   - All items secured by each component security group that you include in the context-sensitive security group.

   Note: Users in security groups that you haven't selected in the **Allows Access to Security Groups** prompt can still submit My Tasks approvals. To restrict access to My Tasks approvals, you must include **Inbox Approvals** in the **Excludes Functionality** prompt.

3. From the **Excludes Functionality** prompt, select the Workday functionality to which you want to restrict access.

Option	Description
Attachment Download (Limited)	Prevents users from viewing and downloading certain attachments that they upload to Workday. Doesn't prevent users from uploading attachments. Examples of attachments that Workday exempts from this functionality exclusion include: • Downloads of attachments on business processes. • Downloads from **My Tasks**. • Payslips. Workday recommends that you test access restrictions that use this functionality exclusion in your Sandbox tenant before you migrate them to your Production tenant. Ensure that your access restrictions prevent users from viewing and downloading attachment types to which you're restricting access.
Business Process Steps Sent Back for Revision	Prevents users from accessing Revise steps sent to **My Tasks** from business processes. Workday displays **Action no longer available** when you access **My Tasks** actions to which this functionality exclusion applies.

Option	Description
Check In/Out	Prevents users from checking in and out directly in Workday using the: • **Time** worklet. • **Check In** and **Check Out** tasks. • Workday mobile apps.
Export to PDF or Excel (Except Payslips and W2s)	Prevents users from exporting documents generated by Workday as PDF or Excel files, except for: • Single payslips. • W-2 forms.
Export to PDF or Excel	Prevents users from exporting any documents generated by Workday as PDF, Excel, or CSV files. When you select **Export to PDF or Excel (Except Payslips and W2s)** or **Export to PDF or Excel** from **Excludes Functionality**, the **Document Type(s) to Exclude** prompt will appear. This prompt enables you to prevent users from downloading all or some of these document classifications from **My Reports**: • *Comma Separated Values (CSV)* • *Compressed Archive (Zip)* • *DOCX Document (DOCX)* • *HTML Document (HTML)* • *JSON Document (JSON)* • *Text Document (TXT)* • *Worksheet (JWF)* • *XML Document (XML)* **Note:** Workday's classification of document types may not match the actual file extension name.
Inbox Approvals	Prevents users from accessing **My Tasks** actions sent to them as the result of these types of business process steps: • *Approval* • *Approval Chain* • *Consolidated Approval* • *Consolidated Approval Chain* • *Review Documents* Workday displays **Action no longer available** when you access **My Tasks** actions to which this functionality exclusion applies. Some business process steps that display an **Approve** button when run aren't subject to this functionality exclusion. Example: A Review Employee Termination *Action* step.

Option	Description
Inbox Complete Actions/To Dos	Prevents users from accessing **My Tasks** actions Workday sends to them as the result of these types of business process steps: • *Checklist* • *To Do* Workday displays **Action no longer available** when you access **My Tasks** actions to which this functionality exclusion applies.
Payment Elections	Prevents users from modifying their self-service payment elections. Doesn't restrict users from viewing their payment elections.

Result

The **Access Restriction** column on the **Signons and Attempted Signons** report contains the names of access restrictions that Workday applies to user sessions.

Related Information
Concepts
Concept: Security Groups on page 129
Tasks
Add Authentication Rules on page 8

Activate Pending Authentication Policy Changes

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can activate pending changes to authentication policies and create an activation timestamp for auditing purposes. When you activate pending authentication policy changes, Workday compares them with your current sign-in method, and doesn't let you activate pending authentication policy changes if they:

- Disallow your current sign-in. Example:
  - You sign in to Workday using user name password authentication.
  - The pending authentication policy changes would disable user name password authentication for your account.
- Subject your Workday account to an access restriction. Example:
  - You sign in to Workday from outside the corporate network.
  - The pending authentication policy changes restrict access to within the corporate network only.

Note: You can't activate multiple authentication policies for the same environment.

Steps

1. Access the **Activate All Pending Authentication Policy Changes** task.
   All authentication policies display, even if an authentication policy has no pending changes. Click the tree control to view each authentication policy and the environments each policy applies to.
2. Enter a **Comment** to describe the changes.
3. Select the **Confirm** check box to activate the changes.

Result

The **Manage Authentication Policies** page displays the current authentication policy evaluation moment and your comment. The most recent changes made to authentication policies since the previous active timestamp take effect immediately. Workday also updates the active timestamp to the current time. You can view the audit trail for any authentication policy from its related actions menu.

Concept: Authentication Policy Best Practices

Authentication Policy Definitions

Authentication policies provide granular control of user authentication. You can define and enable an authentication policy based on:

- Security group membership.
- The networks and devices from which users access Workday.

We recommend that you refine your security settings by defining authentication rules in the **Authentication Allowlist**, rather than only listing Internet Protocol (IP) addresses in the **Network Denylist**. When defining authentication rules, consider:

- Your company policies and internal requirements.
- Strengths and risks of each authentication type, and multifactor authentication type if you use it.
- Implementation effort required to deploy and maintain security.
- Types of users based on their role. We recommend that you use more restrictive authentication for administrators who have a higher level of access. Example: Require multifactor authentication for administrators if you normally require regular authentication for most employees.
- Network restrictions. Example: Workers can only access Workday from the corporate network.
- Access restrictions. Example: Give workers greater access on the corporate network, and only self-service access when they sign in from another network.

Arrange your authentication rules in decreasing levels of restriction. Workday:

- Evaluates rules in the order that you've arranged them.
- Processes only the first rule that applies to the user.

Example: Position a rule for HR administrators before a rule for all workers.

We recommend that you define a default rule for all users. Configure the rule so users who you don't include in any other rule can still sign in to Workday. If you don't define conditions for a default rule, users in the default category might be able to sign in to Workday using any valid authentication type.

Multifactor Authentication

Your best defense against phishing and social engineering attacks in Workday is multifactor authentication. We recommend that you enable multifactor authentication on your authentication policies. Doing so requires users to provide more than 1 type of identity verification to access Workday. Example: Their username and password that they enter on the Workday sign in page, and a one-time passcode they enter from their smartphone.

You can specify multifactor authentication on authentication policies on which you specify these authentication types:

- User name password.
- SAML.
- OpenID Connect.

Workday provides several multifactor authentication types that you can specify on authentication policies. To specify them on authentication policies, you must first enable them on the **Edit Tenant Setup - Security** task. Workday recommends that you enable more than 1 type of multifactor authentication on

authentication policies when possible. Doing so provides your users with alternate methods of multifactor authentication should their primary multifactor authentication type be unavailable.

If you have Workday Central Login (WCL) enabled for Supplier users, we recommend configuring your multifactor authentication settings to send one-time passcodes to users' primary or work email addresses. This enables members of the WCL Enabled Suppliers security group to securely access Workday using WCL.

Delegated Authentication

Note: Workday plans to retire delegated authentication in a future release. We recommend that you use other forms of authentication that we support.

Should your third-party delegated authentication system go offline, you can avoid Workday locking out users by either:

- Exempting at least 2 administrators from delegated authentication. You then require them to sign in using a Workday-managed authentication type on the corporate network.
- Adding an authentication rule. The rule should enable highest-access level security groups to sign in using at least 2 types of authentication. Example:
  - Add Security Assertion Markup Language (SAML) authentication from any network for everyday use.
  - Add user name password authentication from the corporate network for high-priority users.

  The high-priority users can then perform critical tasks when the delegated authentication system is offline.

Sign-Ins

Regularly review these reports:

- **Signons and Attempted Signons**
- **Workday Accounts Currently Locked Out By Excessive Failed Signon Attempts**

Virtual Clean Room (VCR) Restrictions for Workday Implementers

Workday enforces VCR restrictions for your tenant. Certain Workday implementer accounts can sign in to Workday only from a restricted set of Workday IP addresses. When you define rules in your authentication policy, ensure that the rules don't block Workday implementers from accessing Workday. Example: If:

- Your authentication policy requires implementers to access Workday only from your corporate network.
- Your tenant is subject to VCR restrictions.

Workday implementers can't access Workday.

To help define such a nonblocking authentication policy, Workday provides 2 security groups:

- All VCR Restricted Implementers
- All Non-VCR Restricted Implementers

Define the first rule in the authentication policy to apply to the All VCR Restricted Implementers security group and set the allowed networks (under **Authentication Condition**) to *Any*. Since Workday evaluates that rule first, VCR restricted implementers aren't subject to network IP restrictions imposed by subsequent rules that might conflict with the VCR restriction. You can then define additional rules that subject the All Non-VCR Restricted Implementers security group to your desired IP network restrictions. You can also define the rules to have different authentication type restrictions for VCR restricted and non-VCR restricted implementers if you need.

If you want all implementers to access Workday from certain IP ranges, have Workday disable VCR restrictions. You can then set up an authentication rule to define the network IP ranges that all implementers must use to access your Workday tenant.

Related Information
Reference
Feature Release Note: Unified Supplier Portal
Examples
Example: Emergency Sign-In for Administrators on page 89
Example: Virtual Clean Room (VCR) Restricted Implementer Access for IP-Restricted Tenants on page 94

Concept: Authentication Policies

Authentication policies give you control over how you enable users to sign in to Workday under different conditions. Use them to:

- Set up different authentication requirements for different user populations.
- Enable mobile PIN authentication as well as multifactor authentication.

For each authentication policy, you can define:

- The networks from which to block user access.
- Rules that determine how users can access Workday.

When you use access restrictions in an authentication policy, **My Tasks** always displays all values. Workday doesn't filter **My Tasks** to display only the values accessible by the security groups included in the access restriction. You can suppress **My Tasks** by disabling **My Tasks** access in the access restriction.

Use the **Manage Authentication Policies** report to create and manage authentication policies for your tenant. You can set up multiple authentication policies, but you can only enable 1 authentication policy for each environment. The same authentication policy applies to all Workday clients, including Workday mobile solutions. After you create or change authentication policies, you must activate the changes. Workday won't activate any changes that would invalidate your own sign-in.

If you've enabled Workday Central Login (WCL) for Supplier users, you can select **Edit Workday Managed Auth Policy** in the **Manage Authentication Policies** report. This option enables you to set up multifactor, email-based one-time passcodes for WCL users to authenticate their accounts.

Authentication Allowlist

You can define:

- Rules in the **Authentication Ruleset** that apply to selected security groups.
- A rule in **Default Rule for All Users** for users who aren't members of those security groups.

Each authentication rule contains at least 1 authentication condition that Workday evaluates to determine user access. For an authentication condition, you can specify:

- Networks from which users sign in to Workday (**Authentication Conditions** column). You might prefer specifying allowed networks rather than blocking IP ranges (**Network Denylist** field). It's more manageable to enable fewer networks than to block many.
- That the user sign-in is from a managed device (**Device is Managed** check box).
- The way in which users can authenticate to Workday (**Allowed Authentication Types** and **Multi-factor Authentication** columns). OAuth isn't an option for **Allowed Authentication Types** on an authentication policy.
- Restrictions on Workday functionality available to users after they sign in to Workday (**Access Restriction for Authentication Condition** column).

Example: You can set up an authentication rule that:

- Requires users accessing Workday from a public Wi-Fi network to sign in using SAML from managed devices only.
- Limits their access to self-service tasks.

Multifactor Authentication

You can use multifactor authentication on authentication conditions for which you specify the **user name password**, **SAML**, and **OpenID Connect** authentication types. Multifactor authentication requires users to sign in with a specified type of authentication, and either:

- Submit a verification code from an authenticator app.
- Confirm a push notification or voice callback query from Duo authentication.
- Submit a texted or emailed one-time passcode.

You can enable any combination of these multifactor authentication types on authentication policies, enabling users to select among them as their second authentication factor when signing in:

- **Authenticator App**
- **One Time Passcode – Email**
- **One Time Passcode – SMS**

You can also enable **Duo** multifactor authentication on authentication policies, enabling users to use it as their second authentication factor when signing in.

How Workday Processes Authentication Policies

For an authentication policy to apply, the current environment of the user must match an environment selected in the **Restricted to Environment** field on the authentication policy. If the environment doesn't match, Workday proceeds to the next authentication policy until it identifies an active authentication policy for the current environment. If no active authentication policies match the environment, Workday authenticates the user based on tenant settings.

If an authentication policy matches, Workday determines user access in this order:

1. **Network Denylist** section. If a user attempts to sign in to Workday from one of these networks, Workday denies access to the user.
2. **Authentication Allowlist** section. Workday:
   - Evaluates authentication rules in the **Authentication Ruleset** in the order listed, ignoring disabled rules.
   - Applies the first authentication rule that matches the user signing in based on their membership in a **Security Group**.

   Within each authentication rule, Workday evaluates each authentication condition in the order listed. The action taken depends on the selection made in the **Authentication Conditions** field for the condition:

   - **Specific**: Workday checks if the incoming IP address matches any of the IP addresses in the specified ranges. If there's no match, Workday evaluates the next authentication condition. If Workday finds an IP address match *and* any **Allowed Authentication Types** on the condition match, Workday authenticates the user and applies access restrictions if any. If none of the **Allowed Authentication Types** match, Workday evaluates the next authentication condition.
   - **Any**: If the user's method of authentication matches any of the **Allowed Authentication Types**, Workday authenticates the user and applies access restrictions if any. Otherwise, Workday denies access to the user.
   - **Any except other conditions**: If the user's method of authentication matches any of the **Allowed Authentication Types**, *and* their IP address didn't match any of the specified address ranges in previous authentication conditions, Workday authenticates the user and applies access restrictions if any. If the IP address of the user matched any previous specified address ranges, Workday denies access to the user.

   Within a rule, you should order authentication conditions that specify **Specific** IP ranges before any authentication conditions that specify **Any** or **Any except other conditions**. Workday recommends that only 1 of your authentication conditions specifies **Any**. If you include an authentication condition that

specifies **Any except other conditions**, it must be last condition in authentication condition order on the rule.

Once Workday begins evaluating a given rule, if none of the authentication conditions on the rule applies to the user, then Workday doesn't evaluate any other rules and denies access to the user.

Note: Workday recommends that you arrange your authentication rules in decreasing levels of restriction. Example: Position a rule for HR administrators only before a rule for all workers.

How Workday Assesses Time Zone for Authentication Policies

Workday evaluates membership in these security groups using the time zone of the user. Authentication policy rules that reference these security groups become effective at midnight in the time zone in which the user becomes a security group member.

- All Contingent Workers
- All Employees
- All Pre-Contingent Workers
- All Pre-Employees
- All Retirees
- All Trainees
- Contingent Worker as Self
- Employee as Self
- Pre-Contingent Worker as Self
- Pre-Employee as Self
- Retiree as Self
- Terminee as Self

Example: When a hire becomes effective at midnight Japan Standard Time (JST), Workday:

- Stops enforcing the authentication policy for Pre-Employee as Self.
- Begins enforcing the authentication policy for Employee as Self.

Related Information
Tasks
Steps: Set Up Authentication Policies on page 7
Reference
Workday 32 What's New Post: Time Zones
Feature Release Note: Unified Supplier Portal

Multifactor Authentication

Setup Considerations: Multifactor Authentication

You can use this topic to help make decisions when planning your configuration and use of multifactor authentication. It explains:

- Why to set it up.
- How it fits into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What It Is

Multifactor authentication is a method of confirming the identity of a user by requiring more than 1 type of identity verification. When you enable multifactor authentication, users who authenticate with user name password, SAML, and OpenID Connect must provide additional credentials from:

- Something they have. Example: Their mobile device.
- Something they know. Example: Answers to challenge questions.
- Something they are. Example: Their fingerprint or image.

Business Benefits

Multifactor authentication is the most effective way to prevent phishing and social engineering attacks.

Use Cases

You can enable different types of multifactor authentication for different user populations. Examples:

- Protect the accounts of your global workforce against phishing attacks with:
  - Duo.
  - Authenticator app.
  - Emailed and short message service (SMS) one-time passcode multifactor authentication.
- Protect accounts of users who typically possess a basic cell phone with SMS one-time passcode multifactor authentication.
- Protect accounts of users who can't use the other types of multifactor authentication with challenge questions. Example: Field workers in developing countries.

Questions to Consider

Question	Considerations
Do you need to require multifactor authentication for all of your users?	Workday recommends that you enable multifactor authentication in all of your tenants for all users.

Do you want to enable multifactor authentication for different user populations?	• You can use authentication policies to enable different types of multifactor authentication for users in different security groups.
	• You can set up an authentication policy that:
	  • Requires multifactor authentication when users access Workday from outside your corporate network.
	  • Doesn't require multifactor authentication for users who access Workday on your corporate network.

Do you want to enable more than 1 type of multifactor authentication for your users?	For users who authenticate with user name password, SAML, and OpenID Connect, you can enable any combination of these multifactor authentication types: • Authenticator App. • One Time Passcode – Email. • One Time Passcode – SMS. Workday will then prompt the users to enroll the multifactor authentication types you enable.

Question	Considerations
	Note: You can't enable Duo multifactor authentication in combination with the other multifactor authentication types.
Do your users possess mobile devices such as tablets or smartphones?	• You can use Duo multifactor authentication with mobile devices, basic cell phones, and land lines. • You can use authenticator app multifactor authentication with devices that can run mobile apps. • You can use emailed one-time passcode multifactor authentication with devices that can display work or home emails for your users. • You can use SMS one-time passcode multifactor authentication with devices that support SMS text messaging.
Do your users possess basic cell phones, rather than mobile devices?	You can use SMS one-time passcode multifactor authentication with cell phones that support SMS text messaging.
Do you have a global workforce, or do your users travel globally?	• You can deploy Duo, authenticator app, and emailed one-time passcode multifactor authentication globally. • SMS one-time passcode that uses Twilio-based SMS OTP delivery is available in many countries globally. SMS one-time passcode that uses carrier-based SMS OTP delivery is available only where supported by the mobile phone carrier of the user.
Do you have a budget for multifactor authentication?	Duo requires a paid contract with Duo Security.

Recommendations

- To prevent phishing, educate your users on policies your company has in place.
- Set up your authentication policies to enable more than 1 type of multifactor authentication where possible. Enabling more than 1 type of multifactor authentication provides your users with alternates should their primary multifactor authentication type be unavailable.
- Use backup codes if they're available for the type of multifactor authentication you're using.
- If you use challenge questions, train administrators to use questions having answers that:
  - Are difficult to find.
  - Exhibit a high degree of randomness.

  Example: Don't use questions such as:

  - What is your birth year?
  - What is your favorite color?
  - What town did you live in as a child?
- For users who can't use multifactor authentication, set up an authentication policy with an access restriction. The restriction should prevent users from making payment elections when they aren't on the corporate network.

Requirements

Note: You might need to take additional steps to enable SMS one-time passcode that uses Twilio-based SMS OTP delivery, depending on your organization's subscription service agreement. Workday includes Twilio with your subscription service agreement. For more information, see this Community article.

- Train your users on any authenticator apps that you select. Workday doesn't supply or support any authenticator app. You can use any authenticator app that supports the time-based one-time password (TOTP) standard.
- SMS one-time passcode that uses carrier-based SMS OTP delivery requires:
  - You to maintain a configuration for all mobile phone carriers of users across all geographies.
  - Mobile phone carriers to support email to SMS gateway functionality without throttling.
- Emailed one-time passcode requires that users have current email addresses set up on their worker profiles.
- Duo requires a contract with Duo Security.

Limitations

Challenge questions aren't a true form of multifactor authentication, since both factors are something the user knows. Use challenge questions only when you can't use other methods of multifactor authentication, as the other methods are more secure.

Tenant Setup

Except for challenge questions, you must set up multifactor authentication providers in the tenant before you can specify them on authentication policies. Set up multifactor authentication providers on the **Edit Tenant Setup - Security** task in the **Multi-Factor Authentication Settings** section.

Security

Domains	Considerations
In the System functional area: • *Custom Report Creation.* • *Manage: All Custom Reports.*	Enables you to generate reports listing users who don't have the required email addresses in their worker profiles for emailed one-time passcode multifactor authentication.
Manage: Innovation Services in the Innovation Services functional area.	Enables you to set up SMS one-time passcode multifactor authentication that uses Twilio for delivery of SMS OTPs.
In the Contact Information functional area: • *Self-Service: Work Phone.* • *Self-Service: Home Contact.*	Enables users to select or change their phone number for receiving SMS one-time passcodes.
Set Up: Contact Info, IDs, and Personal Data in the Contact Information functional area.	Enables you to configure the mobile device type for use with SMS one-time passcode multifactor authentication.
Set Up: Tenant Setup - Global in the System functional area.	Enables you to configure the phone number format for use with SMS one-time passcode multifactor authentication.
Set Up: Tenant Setup - Security in the System functional area.	Enables you to: • Add multifactor authentication providers to the tenant.

Domains	Considerations
	• Define authentication policies to specify multifactor authentication on user name password, SAML, and OpenID Connect authentication types.
In the System functional area: • *Workday Accounts.* • *Workday Account Monitoring.*	Enables you to view sign-in messages related to multifactor authentication.

Business Processes

No impact.

Reporting

You can track sign-ins to Workday accounts using the **Signons and Attempted Signons** report. The report includes these columns related to multifactor authentication:

- **Requires MFA**.
- **MFA Enrollment**.
- **Multi-factor**.

Integrations

No impact.

Connections and Touchpoints

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Other Impacts

Anticipate situations where a user can't sign in to Workday because of multifactor authentication. Examples:

- A user misplaces or forgets their mobile device.
- A user gets a new smartphone, basic cell phone, or phone number.
- A user doesn't know how to set up multifactor authentication on their device.
- A user changes an email address so it's different from the email address Workday contains in their worker profile.
- You enable emailed one-time passcode multifactor authentication and some users don't have updated email addresses in their worker profiles.
- The email SMS gateway used by a mobile phone carrier is down.
- The Duo service is down.

To address such situations, you can:

- Enable multiple types of multifactor authentication on authentication policies where possible.
- Use the **Edit Workday Account** task to:
  - Exempt specific users from multifactor authentication.
  - Reset multifactor authentication types for the user.

Related Information
Tasks
Steps: Set Up Multifactor Authentication Using Duo Security on page 26
Steps: Set Up Multifactor Authentication Using Emailed One-Time Passcode on page 27
Steps: Set Up Multifactor Authentication Using SMS One-Time Passcode on page 29
Require Challenge Questions at Sign-In on page 32

Steps: Set Up Multifactor Authentication Using Authenticator App

Prerequisites

- Select a third-party authenticator app for your organization that uses the time-based one-time password (TOTP) algorithm to generate verification codes. Workday doesn't provide such an authenticator app.
- Review Setup Considerations: Multifactor Authentication.

Note: Authenticator apps use time as an input to calculate the verification codes used for sign-in. Ensure that the authenticator apps used by your users synchronize with network time to generate the correct codes.

Context

You can configure your tenant to require certain users to sign in to Workday with a verification code, in addition to their designated authentication types. With an authenticator app based on the TOTP algorithm, you can deploy this multifactor authentication globally. You can also configure Workday to generate one-time backup codes for users if their authenticator app is unavailable.

Multifactor authentication doesn't apply to SOAP or REST web service requests.

Steps

1. Access the **Edit Tenant Setup - Security** task.
   On the **Multi-Factor Authentication Providers** grid, click **Add Multi-Factor Authentication Provider** and add these authentication providers to the tenant:
   - **Authenticator App**
   - (Optional) **Backup Codes**

   Security: *Set Up: Tenant Setup - Security* in the System functional area.
2. (Optional) Edit Workday Accounts on page 246.
   Configure multifactor authentication settings for individual users.
3. Add Authentication Rules on page 8.
   Configure rules that require users in certain security groups to sign in to Workday with:
   - Any combination of these authentication types:
     - **User name password**
     - **SAML**
     - **OpenID Connect**
   - **Authenticator App** as a second authentication factor.
   - (Optional) **Backup Codes** as a second authentication factor.

   You can also add certain other types of multifactor authentication on the rules.

Result

Workday automatically prompts users when they sign in to set up the authenticator app.

If you selected backup codes as an authentication factor, Workday displays the backup codes at the end of the setup sequence. Workday recommends that you instruct your users to record their backup codes and store them securely.

Once authenticated, users can access these tasks:

- **Set Up Authenticator App**, to set up another authenticator app. Users can have multiple authenticator apps installed on their devices. They can set up only 1 app to provide multifactor authentication for their Workday accounts at a time, however.
- **Regenerate Backup Codes**, to generate a new set of backup codes, and invalidate existing backup codes.

They can use the **Manage Security Settings** report to access these tasks.

Next Steps

You can review authentication failure messages in the **Signons and Attempted Signons** report.

To reset authenticator app multifactor authentication for a user, necessitating that they set it up again:

1. Access the **Edit Workday Account** task for the user.
2. Select the **Reset** check box for **Authenticator App** in the **Multi-factor Authentication** grid.

Related Information
Reference
Reference: Edit Tenant Setup - Security

Steps: Set Up Multifactor Authentication Using Duo Security

Prerequisites

- An active Duo MFA or higher trusted access plan from Duo Security.
- Integration and secret keys provided by Duo Security to protect the Workday and Admin API applications.
- The unique API hostname provided by Duo Security.
- Review Setup Considerations: Multifactor Authentication.

Context

You can configure your tenant to require that certain users sign in to Workday with:

- Any combination of **user name password**, **SAML**, and **OpenID Connect** authentication.
- Duo multifactor authentication.

Once your users enroll in the Duo service, they can supply the second factor of authentication in the form of:

- Duo Push (response to a push notification).
- Voice callback.
- A one-time passcode, entered from:
  - The Duo Mobile app.
  - A text message.

Use Duo multifactor authentication with user name password, SAML, OpenID Connect, and delegated authentication.

Steps

1. Access the **Edit Tenant Setup - Security** task.

   On the **Multi-Factor Authentication Providers** grid, click **Add Multi-Factor Authentication Provider** and add **Duo** as an authentication provider in the tenant. Duo Security provides the key and hostname information necessary to add the provider. See Reference: Edit Tenant Setup - Security for more information.

   Security: *Set Up: Tenant Setup - Security* in the System functional area.
2. (Optional) Edit Workday Accounts on page 246.

   Configure Duo multifactor authentication settings for individual users.
3. Add Authentication Rules on page 8.

   Define a rule that requires users in certain security groups to sign in to Workday with:

   - Any combination of these authentication types:
     - **User name password**
     - **SAML**
     - **OpenID Connect**
   - **Duo** as a multifactor authentication type.

Result

Workday automatically prompts users through a Duo self-enrollment process when they sign in.

Next Steps

You can review authentication failure messages in the **Signons and Attempted Signons** report.

To reset Duo multifactor authentication for a user, necessitating that they set it up again:

1. Access the **Edit Workday Account** task for the user.
2. Select the **Reset** check box for **Duo** in the **Multi-factor Authentication** grid.

Related Information
Reference
Reference: Signons and Attempted Signons Report on page 96

Steps: Set Up Multifactor Authentication Using Emailed One-Time Passcode

Prerequisites

Review Setup Considerations: Multifactor Authentication.

Context

You can configure your tenant to require certain users to sign in to Workday with:

- Any combination of **user name password**, **SAML**, and **OpenID Connect** authentication.
- A one-time passcode that Workday emails to them.

As this type of multifactor authentication uses email to deliver one-time passcodes to users, you can deploy it globally.

Note: Ensure that you set up email addresses in Workday for users in security groups that you enable for emailed one-time passcode multifactor authentication.

Multifactor authentication doesn't apply to SOAP or REST web service requests.

Steps

1. Access the **Edit Tenant Setup - Notifications** task.

   On the **General Email Notification Settings** grid, ensure that you don't have **Disable All Emails** selected for the environment in which you're configuring this multifactor authentication type.

   Security: *Set Up: Tenant Setup - BP and Notifications* in the System functional area.
2. Access the **Edit Tenant Setup - Security** task.

   On the **Multi-Factor Authentication Providers** grid, click **Add Multi-Factor Authentication Provider** and add the **One Time Passcode - Email** authentication provider to the tenant.

   Security: *Set Up: Tenant Setup - Security* in the System functional area.
3. (Optional) Edit Workday Accounts on page 246.

   Configure multifactor authentication settings for individual users.
4. Add Authentication Rules on page 8.

   Configure rules that require users in certain security groups to sign in to Workday with:

   - Any combination of these authentication types:
     - **User name password**
     - **SAML**
     - **OpenID Connect**
   - **One Time Passcode - Email** as a second authentication factor.

   You can also add certain other types of multifactor authentication on the rules.
5. (Optional) Create an advanced custom report that generates a list of users that:

   - Are in the security groups that you enable for emailed one-time passcode multifactor authentication.
   - Don't have the required email addresses in their worker profiles.

   See Steps: Create Advanced Reports.

   Example: To identify users without a primary work email address in their worker profile, create an advanced custom report that:

   - Uses the **All Workers** data source.
   - Includes these report fields:
     - **First Name + Last Name** on the Worker business object.
     - **User Name** on the Worker business object.
     - **Workday Account** on the Worker business object.
     - **Email - Primary Work** on the Worker business object.
     - **Security Groups** on the Workday Account business object.
   - Has filters that include instances for which:
     - **User Name** isn't blank.
     - **Workday Account** isn't empty.
     - **Email - Primary Work** is blank.
   - Has a subfilter for instances when **Security Groups** are the groups you enabled for emailed one-time passcode multifactor authentication.

6. (Optional) Ensure that you set up email addresses for users in each security group that you enable for emailed one-time passcode multifactor authentication.

   You can use your custom report to identify users without the necessary email addresses. Without email addresses set up in Workday, users won't be able to sign in. Example:

   - You set up the **One Time Passcode - Email** multifactor authentication provider to send one-time passcode emails to work email addresses only.
   - You set up an authentication policy that requires users in the Payroll Administrator security group to authenticate using:
     - Their username and password.
     - An emailed one-time passcode.
   - Norman Chan is a member of the Payroll Administrator security group.
   - He doesn't have a work email address set up on his worker profile.

   He won't receive the one-time passcode Workday requires for him to sign in.

Result

Workday automatically prompts users to verify the email address to which Workday will send one-time passcodes the first time they sign in. If they bypass the setup process, they can set it up by:

1. Accessing the **Set Up One-Time Passcode for Email** task.
2. Selecting the email address to which they want Workday to send one-time passcodes.

Workday then sends an email containing a **Test Passcode** to the designated email address.

Note: Workday doesn't use custom email templates for emailed one-time passcode multifactor authentication.

Users can use the **Manage Security Settings** report to access the **Set Up One-Time Passcode for Email** task.

Next Steps

You can review authentication failure messages in the **Signons and Attempted Signons** report.

To reset emailed one-time passcode multifactor authentication for a user, necessitating that they set it up again:

1. Access the **Edit Workday Account** task for the user.
2. Select the **Reset** check box for **One Time Passcode - Email** in the **Multi-factor Authentication** grid.

Steps: Set Up Multifactor Authentication Using SMS One-Time Passcode

Prerequisites

Review Setup Considerations: Multifactor Authentication.

Note: You might need to take additional steps to enable SMS one-time passcode that uses Twilio-based SMS OTP delivery, based on your organization's subscription service agreement. To determine your subscription service agreement:

1. Access your profile avatar on Community.
2. Select **Profile**.
3. On your profile page, select your organization's name, which is beneath your name and next to your job profile.
4. View your **Subscription Service Agreement** value.

If the value is:

- *MSA*, you might need to enable Twilio-based SMS OTP multifactor authentication through Innovation Services using the **Enable Innovation Services Feature and Machine Learning Data Contributions** step.
- *UMSA*, you can skip the optional **Enable Innovation Services Feature and Machine Learning Data Contributions** step.

Context

You can configure your tenant to require certain users to sign in to Workday with:

- Any combination of user name password, SAML, and OpenID Connect authentication.
- A one-time passcode that they receive in a Short Message Service (SMS) text message.

Workday provides 2 methods for delivering SMS one-time passcodes (OTPs) to users:

- Twilio-based, which uses Twilio Messaging as the delivery service for SMS OTPs.
- Carrier-based, which uses mobile phone carriers to deliver SMS OTPs.

If you don’t enable Twilio-based delivery, Workday uses carrier-based delivery for all users.

Note: You might need to take additional steps to enable Twilio-based SMS OTP multifactor authentication, depending on your organization’s subscription service agreement. Workday includes Twilio with your subscription service agreement. For more information, see this Community article.

SMS one-time passcode authentication:

- Is available for workers and certain nonworker types, such as Implementers or Service Center Representatives.
- Doesn't apply to SOAP or REST web service requests.

Steps

1. (Optional) Edit Domain Security Policies on page 200.

   To enable users to select or change the phone number they use to receive passcodes, grant the Employee As Self security group view and modify access to:

   - The *Self-Service: Work Phone* domain in the Contact Information functional area.
   - (Optional) The *Self-Service: Home Contact* domain in the Contact Information functional area.
2. Verify that you've configured the mobile phone device type for your tenant.

   See Steps: Set Up Phone Numbers.
3. (Optional) Enable Innovation Services Feature and Machine Learning Data Contributions.

   Note: Workday doesn't support Twilio-based SMS one-time passcode delivery in the countries listed in Reference: Twilio-Based SMS OTP Multifactor Authentication Support. If you have users in any of the listed countries, or if they have phone numbers in those countries, ensure you also enable emailed delivery of one-time passcodes. Twilio-based SMS won't work in those countries, but you can still use Twilio for the rest of your users. See Steps: Set Up Multifactor Authentication Using Emailed One-Time Passcode.

   Select the **SMS Multi-factor Authentication** service in the **Cross Application Services** category.

4. (Optional) Access the **Edit Tenant Setup - Security** task.

   On the **Multi-Factor Authentication Providers** grid:

   a. Click **Edit** for the **One Time Passcode – SMS** multifactor authentication provider.
   b. Add carrier information for the mobile phone carriers that your users use.
   c. Select the **Allow Home Mobile For One Time Passcode** check box to enable users to select phone numbers from the **Home Contact Information** in their profile to receive SMS one-time passcodes.

   You can't enter carrier information if you enabled Twilio-based OTP delivery.

   See Reference: Edit Tenant Setup - Security.

   Security: *Set Up: Tenant Setup - Security* in the System functional area.
5. (Optional) Configure SMS one-time passcode authentication settings for individual users.

   See Edit Workday Accounts on page 246.
6. Add Authentication Rules on page 8.

   Configure rules that require users in certain security groups to sign in to Workday with:

   - Any combination of these authentication types:
     - **User name password**
     - **SAML**
     - **OpenID Connect**
   - **One Time Passcode - SMS** as a second authentication factor.

   You can also add certain other types of multifactor authentication on the rules.
7. (Optional) Enable one-time passcode authentication for certain nonworker account types, such as Implementers or Service Center Representatives.

   You can do so if the account has the required contact information and it has access through the appropriate domain. Example: For a Service Center Representative:

   - Verify that the account has the required contact information.
   - Grant the Service Center Representative as Self security group view and modify access to the *Self-Service: Service Center Representative* domain.

Result

Workday automatically prompts users to set up SMS one-time passcode when they sign in. During setup, users select a mobile carrier. They also select, from a list of numbers, the mobile number to which Workday sends them SMS one-time passcodes:

- If you didn't select the **Allow Home Mobile For One Time Passcode** check box on **Edit Tenant Setup - Security**, only work numbers in their user profile display in the list.
- If you selected **Allow Home Mobile For One Time Passcode**, then all work numbers in their profile display first, followed by the home numbers.

If they have more than 1 work or home number set up in their profile, then the order in which they display in the list is random.

If they bypass the setup process, they can set it up by:

1. Accessing the **Set Up One-Time Passcode for SMS** task. Users can use the **Manage Security Settings** report to access the **Set Up One-Time Passcode for SMS** task.
2. Selecting their phone number and mobile carrier for receiving passcodes.

Workday sends a text message containing a **Test Passcode** to their designated mobile phone.

Next Steps

You can review failure messages for SMS one-time passcode authentication in the **Signons and Attempted Signons** report.

To reset SMS one-time passcode multifactor authentication for a user, necessitating that they set it up again:

1. Access the **Edit Workday Account** task for the user.
2. Select the **Reset** check box for **One Time Passcode - SMS** in the **Multi-factor Authentication** grid.

Manage Challenge Questions

Prerequisites

Note: Workday plans to retire challenge questions in a future release. We recommend that you use other forms of authentication that we support.

Security: *Security Administration* domain in the System functional area.

Context

Manage tenant-wide challenge questions. Workday prompts users for their answers to these questions if you:

- Configure your authentication policy to require users to answer challenge questions when they sign in to Workday.
- Enable users to reset their password online or through email.

You must have at least 5 challenge questions active in the tenant. The number of these challenge questions that your users need to set up and use depends on when Workday requires them. If you configure Workday to require challenge questions to:

- Sign in to Workday only, users need to set up and use 2 of the challenge questions.
- Reset forgotten passwords online only, users need to set up and use 3 of the challenge questions.

If Workday requires challenge questions to sign in and reset forgotten passwords online, users must set up 5 challenge questions.

Steps

1. Access the **Maintain Tenant Challenge Questions (Do Not Use)** task.
2. Add rows for new questions.

   You can modify existing questions that you add, but not the questions that Workday provides.
3. Set the **Order** for the questions.
4. Select the **Active** check box for the questions to list on the **Manage Password Challenge Questions (Do Not Use)** task. Activate at least 5 questions.

Related Information
Tasks
Configure Password Reset on page 253
Steps: Set Up Authentication Policies on page 7

Require Challenge Questions at Sign-In

Prerequisites

Note: Workday plans to retire challenge questions in a future release. We recommend that you use other forms of authentication that we support.

- Review setup considerations for multifactor authentication.
- Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can require users in selected security groups to answer challenge questions when they sign in to Workday. Workday provides 10 challenge questions. You can use the **Maintain Tenant Challenge Questions (Do Not Use)** task to modify them and to add your own questions. Maintain at least 5 active questions. If you use challenge questions for sign-ins and not for forgotten passwords, Workday only uses 2 of these questions and ignores the rest.

Challenge questions don't apply to users who use SAML authentication, nor do they apply to SOAP or REST web service requests.

Steps

1. Access the **Edit Authentication Policy** task.
2. In the **Authentication Allowlist** section, under **Authentication Ruleset**, add an authentication rule.
3. Under **Security Group**, add the security groups for which you want to require authentication using challenge questions.
4. Add a condition to the authentication rule.
   a) Under **Authentication Condition**, select the networks from which the selected security groups can sign in to Workday.
   b) Under **Allowed Authentication Types**, select **User Name Password + Challenge Questions (Do Not Use)**.

Result

Workday prompts users in the selected security groups to set up their challenge questions and answers the next time they sign in to Workday. They must set up the questions and answers even if they previously set up challenge questions for password reset. For subsequent sign-ins, they must enter their username and password, and answer 2 challenge questions. Workday locks user accounts after multiple failed sign-in attempts.

Related Information
Tasks
Add Authentication Rules on page 8
Reference
Setup Considerations: Multifactor Authentication on page 20

Reference: Twilio-Based SMS OTP Multifactor Authentication Support

Workday supports Twilio Messaging as the delivery service for SMS one-time passcode multifactor authentication in many countries. However, Workday doesn't support Twilio Messaging as the delivery service in the countries listed below. If your users reside in one of these countries or have phone numbers in these countries, also enable emailed delivery of one-time passcodes. Twilio-based SMS won't work in these countries, but you can still use Twilio for the rest of your users.

- Afghanistan
- Algeria
- Angola
- Azerbaijan
- Bangladesh
- Benin
- Bhutan
- Brunei
- Burkina Faso
- Burundi
- Cambodia

- Cameroon
- Cape Verde
- Central Africa
- Chad
- Comoros
- Congo
- Cuba
- Djibouti
- East Timor
- Egypt
- Equatorial Guinea
- Eritrea
- Ethiopia
- Falkland Islands
- Gabon
- Gambia
- Ghana
- Guinea
- Indonesia
- Iran
- Iraq
- Israel
- Ivory Coast
- Lesotho
- Liberia
- Libya
- Malawi
- Mali
- Mauritania
- Mozambique
- Nigeria
- Oman
- Pakistan
- Palestinian Territory
- Paraguay
- Reunion/Mayotte
- Sao Tome
- Senegal
- Sierra Leon
- Somalia
- South Sudan
- Sri Lanka
- Sudan
- Syria
- Tajikistan
- Tanzania
- Togo
- Tunisia
- Turkiye
- Turkmenistan

- Uganda
- Vietnam

Step Up Authentication

Steps: Configure Step Up Authentication

Context

You can configure step up authentication to require a second level of authentication to access certain restricted items.

Steps

1. Access the **Edit Tenant Setup - Security** task.

   Select the **Enable SAML Authentication** check box in the **SAML Setup** section.

   Security: *Set Up: Tenant Setup - Security* in the System functional area.
2. Set up a SAML Identity Provider (IdP) to use for service provider-initiated SAML authentication, which Workday needs for step up authentication.

   See Configure Identity Provider-Initiated and Service Provider-Initiated SAML Authentication on page 47.
3. Add Authentication Rules on page 8.

   Add or edit authentication rules on an authentication policy to enable SAML authentication for security groups that need to access a privileged session.
4. Create Step Up Authentication on page 35.
5. Activate Pending Authentication Policy Changes on page 15.

Next Steps

View the **Signons and Attempted Signons** report to monitor privileged sessions, marked *Step Up Authentication – SAML* in the **Authentication Type for Signon** column.

Related Information
Concepts
Concept: Step Up Authentication on page 36

Create Step Up Authentication

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can create a step up authentication configuration. Step up authentication requires users to sign in to a privileged session before they can access restricted items that you specify.

Steps

1. Access the **Add Authentication Policy** or **Edit Authentication Policy** task from the **Manage Authentication Policies** report.
2. In the **Step Up Configuration** prompt, click **Create Step Up Configuration**.

3. As you complete the task, consider:

Option	Description
Security Groups Exempted	Users in exempted security groups don't need to enter a privileged session to access items restricted by step up authentication. You can only add unconstrained or context-free security group types. **Note:** Users in security groups that don't have Security Assertion Markup Language (SAML) access in the tenant authentication policy won't be able to enter a privileged session. Either exempt those security groups from step up authentication, or provide them with SAML access in an authentication policy.
Context for Step Up	The authentication context that describes the method that Workday requests the IdP use for authentication during step up. Obtain the authentication context URI from the IdP you're using for step up authentication, and enter it exactly into this field. Example: urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTra
Default IdP	If a user doesn't use SAML to sign in to Workday, Workday uses the IdP you configure on the **Edit Tenant Setup - Security** task for step up authentication. The IdP you select here must be configured for SP-initiated SAML authentication.

4. On the **Business Process Types** tab, select business process types to add as restricted items. Workday displays only functional areas that have a valid selectable domain.
5. On the **Domains** tab, select the domains that secure the tasks that you want to add as restricted items. For each domain:
   - **Step Up for Modify Only**: Users can view information on the task but can't modify information on the task until they enter a privileged session.
   - **Step Up for View and Modify**: Users can't view or modify information on the task until they enter a privileged session.
6. On the **Sensitive Data Groups** tab, select data groups to add as restricted items. Workday prompts users to step up when the sensitive fields in a selected data group display in a task, or a standard or custom report.

Next Steps

To edit an existing step up configuration, select it in the **Step Up Configuration** prompt. Click **See in New Tab**, then select **Step Up Configuration** > **Edit** as a related action.

Concept: Step Up Authentication

Step up authentication requires an additional level of verification for users to access restricted items in your tenant. When a user signs in with step up authentication, Workday creates a privileged session that enables access to the restricted items. Use step up authentication if your security or compliance team determines that certain items in your Workday tenant require additional user verification. Example: Report fields containing Person Global Identifiers like social security numbers.

When you configure step up authentication, you must specify the:

- Security Assertion Markup Language (SAML) identity provider (IdP).
- Privileged session duration.
- Restricted items.

SAML IdP

SAML is the only authentication type that Workday supports for step up authentication. If a user signs in to Workday using:

- SAML, then Workday uses the SAML IdP of that session when the user signs in to access restricted items.
- Another method (Example: user name and password), then Workday uses the default IdP that you configured.

Note: The IdP that Workday uses for step up authentication must be configured for SP-initiated SAML.

Workday step up authentication SAML requests use these attributes to require user credentials at each authentication request in an IdP session:

- *Authentication Context Class Reference*: You obtain the URI of the authentication context class from the IdP and specify it during step up configuration.
- *Force AuthN flag*: Workday automatically populates this value as *True*.

Your IdP must recognize these attributes for proper step up authentication operation.

Privileged Session Duration

You can configure the duration of the initial privileged session as well as the session extension. Workday recommends that you set the initial session and extension times to the average time it takes for the longest running restricted task to complete.

Restricted Items

You configure which items require a privileged session to access by adding their domains, business process types, or sensitive data groups to the step up configuration. These items include:

- Tasks.
- Reports.
- Data sources and data source filters.
- Report fields.
- All business process actions.
- Data fields, such as Person Global Identifier, in a sensitive data group.

Non-Proxy and Proxy User Authentication

These requirements for step up apply to the **Business Process Types**, **Domains**, and **Sensitive Data Groups** tabs on the step up configuration page.

User Type	Step Up Requirements
Non-Proxy User	A user must reauthenticate, unless: • The user is part of a step-up-authentication-exempted security group. • You've configured the sensitive data group and the processing user account for masking. Workday doesn't initiate step up for data that you've already masked.

User Type	Step Up Requirements

	If you haven't configured the sensitive data group for step up, Workday won't require the user to reauthenticate, unless:
	• Workday secures the data element by a domain that you've configured for step up.
	• The data element is visible using an action on a business process type that you've configured for step up.
	Workday requires a user to reauthenticate only once when:
	• Workday has the field secured by a domain security policy.
	• The field is accessible using a business process configured on these tabs on the step up configuration page:
	  • **Domains**
	  • **Business Process Types**

Proxy User	Workday requires a proxy user to reauthenticate when they are: • In a step-up-exempted security group and proxy in as a user who isn't in a step-up-exempted security group. • Not in a step-up-exempted security group and proxy in as a user who isn't in a step-up-exempted security group. Workday doesn't require proxy users to reauthenticate when they proxy for a user for whom Workday masks accessed data.

Step Up Authentication Policy

You configure step up authentication by security groups. Configure your authentication policy to enable SAML authentication for security groups that will need to enter into a privileged session. You can, however, exempt certain security groups from step up authentication. Users in exempted security groups can access restricted items without entering a privileged session.

Authentication Selectors

Set Up Authentication Selectors

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can use authentication selectors to present more than 1 authentication option on a custom sign-in page.

Steps

1. Access the **Manage Authentication Selectors** report and click **Add Authentication Selector**.
2. Complete 1 row in the **Redirection URLs** grid for each redirect link.

   Consider the order that you want links to display on the sign-in page as you enter information in the **Redirection URLs** grid. You can't reorder rows in the grid.
3. As you complete the task, consider:

Option	Description
Name	Workday uses this name as the redirect link on the sign-in page.
Login Redirect URL	Workday redirects unauthenticated users to this URL when they sign in to Workday on a desktop browser.
Mobile App Login Redirect URL	Workday redirects unauthenticated users to this URL when they sign in to Workday on: • Android • iPad • iPhone
Mobile Browser Login Redirect URL	Workday redirects unauthenticated users to this URL when they sign in to Workday on a mobile browser.

Next Steps

Select authentication selectors for use in the **Redirect Type** field of the **Redirection URLs** grid on the **Edit Tenant Setup - Security** task.

Use the **Translate Business Object** report to add translations for the **Name** and **Description** attributes on the **Redirection URL** business object.

Related Information
Tasks
Translate Business Data
Reference
Reference: Edit Tenant Setup - Security

Trusted Devices

Steps: Set Up Trusted Devices

Context

You can set up trusted devices to provide an extra layer of security for users, providing them with real-time information they can use to protect their accounts. Trusted devices reduces vulnerability to phishing and social engineering attacks. It enables users to react quickly if they suspect someone is accessing their account from a device they don't trust.

Trusted devices can also enable users to access their accounts after lockout due to malicious behavior, such as from Denial of Service attacks. If Workday locks an account because of multiple sign in attempts with incorrect passwords from a device that a user doesn't trust, the user can still sign in and access their account from a trusted device.

You can enable trusted devices for these authentication types in Workday:

- User name password.
- Security Assertion Markup Language (SAML).
- Passwordless sign-in.
- OpenID Connect (OIDC).
- Delegated authentication.

Trusted devices doesn't change the authentication method users use to sign in to Workday.

Steps

1. Access the **Edit Tenant Setup - Security** task and clear the **Disable Trusted Devices** check box if it's selected.

   Security: *Set Up: Tenant Setup - Security* domain in the System functional area.
2. Select the **Enable Security Emails** check box and select an appropriate delivery option.

   See Reference: Edit Tenant Setup - Security.
3. Access the **Edit Tenant Setup - Notifications** task.

   Security: *Set Up: Tenant Setup - BP and Notifications* domain in the System functional area.
4. On the **General Notification Restrictions** grid, ensure that you don't have any restrictions configured for the *Email* channel.
5. (Optional) Ensure that your users are members of the *Self-Service: Security Actions* domain in the System functional area, so they have access to the **Manage Trusted Devices** report.

   The *Self-Service: Security Actions* domain is a subdomain of the *Self-Service: Account* domain. See Edit Domain Security Policies on page 200.
6. (Optional) Create an advanced custom report that generates a list of users that don't have the required email addresses in their worker profiles.

   See Steps: Create Advanced Reports.

   Example: To identify users without a primary work email address in their worker profile, create an advanced custom report that:

   - Uses the **All Workers** data source.
   - Includes these report fields on the Worker business object:
     - **First Name + Last Name**.
     - **User Name**.
     - **Workday Account**.
     - **Email - Primary Work**.
   - Has filters that include instances for which:
     - **User Name** isn't blank.
     - **Workday Account** isn't empty.
     - **Email - Primary Work** is blank.
7. (Optional) Ensure that you set up email addresses for users so that they'll receive trusted device emails.

   You can use your custom report to identify users without the necessary email addresses. Without the email address, they won't receive trusted device emails. Example:

   - You set up the **Enable Security Emails** delivery option to **Send to work email only**.
   - Norman Chan doesn't have a work email address set up on his worker profile.

   He won't receive the trusted device email.

Result

Users receive email notifications from Workday when someone signs in to their account from a device that they haven't registered as a trusted device. If a user skips trusting a device, Workday will ask them again if they want to trust it on their next sign-in.

Next Steps

Users can view a list of the devices they've trusted, and remove devices from that list, using the **Manage Trusted Devices** report. They can use the **Manage Security Settings** report to access the **Manage Trusted Devices** report. Users must be members of the *Self-Service: Security Actions* domain to access the report.

Concept: Trusted Devices

The trusted devices feature enables users to take action if they suspect unauthorized access to their account. Users receive an email notification from Workday when a sign-in occurs to their account on a device that they haven't trusted. They can then notify their security administrator and change their password if they suspect someone has compromised their account.

Trusted devices is a tenant-wide feature. You can't configure it for specific groups of users.

What Workday Considers to Be a Trusted Device

Workday considers a unique device that users can trust to be a combination of:

- A hardware device. Example: A computer, tablet, or mobile device.
- A browser.

Example: A user signing in to Workday on a Mac OS computer using the Chrome browser is a device that they can trust. The same user signing in to Workday on the same Mac OS computer using the Safari browser is another device that they can trust.

For users signing in to Workday on mobile devices, Workday considers the mobile browser and mobile app to be different devices.

When a user chooses to trust a device, Workday stores the trust information in a browser cookie. When the user signs in from the same device and browser, Workday determines if it trusts the device based on the presence of trust information in the cookie.

Workday will, however, prompt the user to trust a device again even if they've already trusted it when:

- They're using a shared device that clears all user session information every time they sign out.
- Their browser preferences are set to block cookies for specific sites or clear cookies when the browser closes.
- They're using a private or incognito browser page.
- Your company enforces a browser cookie policy that deletes cookies when users sign out.
- You have SAML Single Sign-On configuration that clears the browser cache and cookies based on **Logout Redirect URL** settings.

Account Lockout Mitigation

Trusted devices can enable legitimate users to access accounts that Workday locks due to too many incorrect sign-in attempts, such as from Denial of Service attacks. When multiple sign-in attempts are made to a Workday user account, and the:

- Device on which the access attempts are made isn't a trusted device.
- Number of attempts exceeds the **Failed Signon Attempts Before Lockout** setting on the **Maintain Password Rules** task.

Workday locks the account for the duration of the **Lockout Minutes** setting.

Legitimate owners of the account, however, still have 20 attempts to authenticate from a trusted device. If they successfully authenticate within 20 attempts from a trusted device, Workday successfully signs them in and unlocks the account. If they don't successfully authenticate within 20 attempts, however, Workday locks the account for the specified lockout period, and removes the device as a trusted device. Users will need to trust the device again the next time they sign in.

Trust Period

Workday trusts a device for 180 days, with the time period resetting each time the user successfully signs in. If a user hasn't signed in from a given trusted device for 180 days, the trust period for that device expires. The user will need to trust the device again the next time they sign in.

Trusted Device Emails

Trusted devices doesn't use Workday email templates, so you can't change the content of the notification emails. Workday does, however, support translation of email notifications to all languages we support.

SAML

Setup Considerations: SAML SSO

You can use this topic to help make decisions when planning your configuration and use of Security Assertion Markup Language (SAML) authentication for Single Sign-On (SSO). It explains:

- Why to set it up.
- How it fits into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What It Is

SAML SSO enables users to authenticate once and securely access Workday and other applications. SAML is the most common standard used by organizations for SSO, enabling you to configure authentication messaging between service providers (SPs) like Workday and Identity providers (IdPs).

Business Benefits

- Reduction in manual effort on the part of your users to manage different credentials for individual applications.
- Reduced support calls related to misplaced or hacked passwords.
- Reduced administrative costs by centralizing user identity and account management tasks.
- Wide acceptance of the open SAML standard by many IdPs and applications like Workday for SSO.

Use Cases

- Users at a company can supply their user credentials once and then access Workday and their other applications without signing in for the rest of their work day.
- The security administrator at a company can revoke access to all users centrally while identifying a security breach, then centrally restore access once they resolve the issue.

Questions to Consider

Questions	Considerations
How do you want users to sign in to your applications?	You can configure: • IdP-initiated SAML, enabling users to access 1 URL, the URL of the IdP, to initiate SSO. Users then access their applications from a page provided by the IdP. • SP-initiated SAML, enabling users to initiate SSO by accessing the URL of the application they want to access. The application then sends an authentication request to the IdP, which: **1.** Authenticates the user. **2.** Enables access to the application. **3.** Returns the user to the application. Workday supports only 1 IdP in a tenant environment for SP-initiated SAML. Consider using SP-initiated SAML when your IdP doesn't supply a user-accessible sign-in page.
Do you use or want to configure multifactor authentication?	You can configure multifactor authentication from: • Your IdP, enabling you to use multifactor authentication on all of your applications that use SSO. • Workday. You can use Workday-provided multifactor authentication if your IdP doesn't support it. When you use Workday-provided multifactor authentication, consider enabling it individually for each of your other applications that use SSO.
Do you want to consider the managed device status of your devices as a condition for accessing Workday?	A managed device in this context is a device that a third-party mobile device management (MDM) provider administers for your organization. You can use SAML on authentication policies to enable Workday access based on whether or not devices are managed devices. Example: Users can: • Have unrestricted access to Workday when they sign in from a company-issued laptop or smartphone. • Access only self-service tasks when they sign in from their personal laptop or smartphone. To configure this functionality, use a Mobile Device Management (MDM) solution with your IdP. Your: • MDM solution must identify the hardware devices that users use to sign in. It identifies these devices by maintaining an updated list of managed devices with the MDM. • IdP must pass messages to the MDM service, process responses from the MDM service, and

Questions	Considerations
	send a managed device attribute to Workday in the SAML response.
How do you want to configure sign-out behavior?	You can separately configure 2 types of SAML single logout (SLO): • Workday-initiated logout, where Workday sends a SAML logout request to the IdP when users sign out at Workday. The IdP then signs the user out at itself and at all other applications associated with the SSO session. • IdP-Initiated logout, where the IdP sends a logout request to Workday, which signs the user out of Workday, when users sign out at the IdP.

Recommendations

- Check if your IdP has a preconfigured user provisioning solution with Workday. Workday has standard development methodology in place with several large SSO vendors (Examples: Okta and Microsoft Azure) for provisioning. When you don't implement user provisioning, you must manually synchronize user information between the IdP and Workday.
- Check if your IdP has any companion documentation describing how to connect Workday to their system.
- Check if your IdP has an IdP metadata XML file available, and upload it to your tenant to configure the IdP setup in Workday automatically.
- Ensure that at least 1 security administrator can access Workday if the IdP goes offline. Example: Configure an authentication rule that enables security administrator access over your corporate network using user name password and multifactor authentication.
- If you configure SP-initiated SAML, ensure that you've configured the Mobile Browser Login redirect URL correctly. Doing so ensures that SAML functions correctly with all devices that your users use to access Workday. You can set the Mobile Browser Login redirect URL to the same value as the Login Redirect URL if you don't have a unique mobile browser URL.
- Configure SAML SLO if your IdP and applications support it. SAML SLO helps reduce or eliminate orphaned active user sessions, which are sessions that still exist at the IdP or Workday after sign-out. They can enable users to create a new Workday session without entering credentials.

Requirements

- Your IdP must support SAML 2.0 and use the SAML 2.0 HTTP POST binding.
- Your IdP must sign the entire SAML message it sends to Workday.
- User names that the IdP passes to Workday must exactly match the username attribute that Workday has configured on the user account.
- The IdP must include these elements in SAML response messages that it sends to Workday:
  - *Conditions*
  - *Destination*
  - *Issuer*
  - *Signature*
  - *Subject*
- Step-up authentication uses SAML. The IdP you use for step-up authentication must recognize the Authentication Context Class Reference or the ForceAuthN=true flag. Step-up authentication only works with SP-initiated SAML.

Limitations

- Workday doesn't support SAML encryption.
- You can only configure 1 IdP for a tenant environment for use with SP-initiated SAML.

Tenant Setup

You configure SAML SSO on the **Edit Tenant Setup - Security** task.

Security

These domains in the System functional area:

Domains	Considerations
Set Up: Tenant Setup - Security	Enables you to configure IdPs and SSO redirect URLs in Workday.
Security Administration	Enables you to: • Create X.509 private key pairs that Workday uses to sign SAML sign-out requests. • Save X.509 public certificates, supplied by the IdP, in Workday. Workday uses X.509 certificates to verify the signature on SAML sign-in and sign-out requests. • Decode and validate SAML messages that Workday receives from IdPs.
Workday Accounts *Workday Account Monitoring*	Enables you to monitor SAML signon activity using the **Signons and Attempted Signons** report.

Business Processes

No impact.

Reporting

Reports	Considerations
Signons and Attempted Signons	Enables you to monitor authentication events, including SAML authentication.
Validate SAML Message	Enables you to validate and troubleshoot SAML response messages sent from the IdP to Workday.

Integrations

Integrations or Web Services	Considerations
Okta - Worker	You can use this template in an Okta integration to enable real-time synching of worker profiles from Workday to Okta. Such integrations enable certain Workday business processes and transaction events to trigger Okta to retrieve changes to worker data using Workday Web Services APIs.

Integrations or Web Services	Considerations
Account Provisioning *Account Provisioning Connector: Worker*	You can use these integration templates to configure user provisioning.

Connections and Touchpoints

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Related Information
Concepts
Concept: SAML Authentication on page 61
Concept: Configuring Your SAML Provider on page 56

Steps: Set Up SAML Authentication

Prerequisites

- Understand the Security Assertion Markup Language (SAML) 2.0 specification and how SAML works.
- Work with your SAML provider to set up the identity providers (IdPs) for Workday to use for SAML authentication.
- Synchronize Workday user names with the user names at your SAML provider. The sign-in ID that your IdP passes to Workday must correspond to a valid Workday account.

Context

You can enable users to sign in to Workday using SAML identity providers by setting up SAML authentication. Workday supports:

- Identity provider-initiated SAML: Users access the URL of the IdP to sign in, then access Workday as authenticated users from a page provided by the IdP.
- Service provider-initiated SAML: Users access the Workday URL, Workday redirects them to the IdP to sign in, and they return to Workday as authenticated users.

Some large SAML vendors (Examples: Okta and Microsoft Azure) might provide documentation that details information such as parameters needed from Workday to configure their IdPs, and IdP parameters needed by Workday. Check with your SAML vendors to determine if they provide such documentation or other information.

Steps

1. Obtain this information from your SAML provider for each IdP you're setting up in Workday. If your SAML provider has IdP metadata XML files available for the IdPs, obtain them, as they might contain this information:
   - **Issuer**: Unique identifier for the IdP.
   - **x509 Certificate**: Public certificate for validating digital signatures.
   - **IdP SSO Service URL**: URL to which Workday sends SAML authentication requests.
   - **Logout Request URL**: URL to which Workday sends SAML logout requests. You need this information only if you configure Workday-initiated single logout (SLO).
   - **Logout Response URL**: URL to which Workday sends logout responses. You need this information only if you configure IdP-initiated single logout.
2. Access the **Edit Tenant Setup - Security** task.

   Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

3. In the **SAML Setup** section, select the **Enable SAML Authentication** check box.

   Enabling SAML authentication doesn't disable other authentication types already enabled for your tenant.
4. Configure Identity Provider-Initiated and Service Provider-Initiated SAML Authentication on page 47.
5. (Optional) Configure SAML Single Logout on page 51.
6. (Optional) Enable Single Sign-On (SSO) for Mobile

   Configure mobile-specific SAML settings for Workday mobile apps.
7. (Optional) Require users to sign in to Workday using SAML authentication, and include multifactor authentication when available.

   You can create an authentication policy so that certain security groups must sign in to Workday using:

   - SAML.
   - Specific SAML IdPs.

   See Steps: Set Up Authentication Policies on page 7.
8. (Optional) Hide Password Management Tasks on page 52.

Next Steps

Use the **Signons and Attempted Signons** report to monitor SAML authentication for your tenant.

Related Information
Concepts
Concept: SAML Authentication on page 61
Concept: Configuring Your SAML Provider on page 56
Reference
Reference: Edit Tenant Setup - Security
Reference: Signons and Attempted Signons Report on page 96

Configure Identity Provider-Initiated and Service Provider-Initiated SAML Authentication

Prerequisites

- Enable Security Assertion Markup Language (SAML) authentication for your tenant.
- Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can support different user populations with different identity providers (IdPs) by configuring 1 or more SAML IdPs for 1 or more environments. Example: A globally dispersed company uses 1 IdP to authenticate workers in the U.S. and another IdP for workers in Australia.

You can configure IdP settings and SAML redirect URLs in Workday for IdP-initiated and optional SP-initiated SAML authentication. Workday supports only 1 active IdP per environment for SP-initiated SAML.

Steps

1. Access the **Edit Tenant Setup - Security** task.
2. (Optional) If you have IdP metadata XML files for the IdPs you want to use for SAML authentication, then for each file, click **Import Identity Provider**.
3. For each file, enter a unique **Identity Provider Name**, select the environments, and upload the file to the tenant.
4. Add rows to the grid manually for IdPs for which you don't import metadata files.

5. Complete the **SAML Identity Providers** grid for each IdP you want to use.

   If you import a metadata XML file for an IdP, Workday automatically completes certain fields in the grid for that IdP. You'll need to complete some fields manually, however.

Option	Description
Identity Provider Name	Identifies the IdP on the **Signons and Attempted Signons** and **Manage Authentication Policies** reports.
Issuer	Enter the unique identifier for your SAML IdP, which must match the Issuer ID in SAML messages that the IdP sends. You can get this identifier from your IdP.
x509 Certificate	Select or create the X.509 public certificate to use to verify the signature on SAML sign-in and sign-out requests. You can get this information from your SAML provider. See Create an X.509 Public Key for information on using the **Create x509 Public Key** task to save certificates in Workday.
SP Initiated	(SP-Initiated SAML only) Select to specify SP-initiated SAML authentication for the environment selected in the **Used for Environments** field.
Service Provider ID	(SP-Initiated SAML) Identifies Workday as the service provider in the Issuer element of SAML messages sent to the IdP. **Note:** You also must provide the **Service Provider ID** if you configure Workday-initiated single logout. See Configure SAML Single Logout.
Sign SP-initiated Request	(Optional; SP-Initiated SAML only) Workday signs authentication request messages with the private key (**x509 Private Key Pair**). You need to provide the public key to your SAML providers.
Do Not Deflate SP-initiated Request	(Optional; SP-Initiated SAML only) Select this check box to ensure that Workday doesn't deflate the message again if the IdP deflates the authentication request message.
Always Require IdP Authentication	(Optional; SP-Initiated SAML only) Select the check box and 1 of these options: • **ForceAuthn Only**: Forces users to authenticate with their IdP, even if they still have a valid Single Sign-On session with their IdP. • **ForceAuthn and RequestedAuthnContext**: Forces the user to authenticate with their IdP, and ensures that the RequestedAuthnContext element is honored. The RequestedAuthnContext element specifies the desired authentication methods. The forced authentication, therefore, will accept only the specified authentication methods when the SAML request is

Option	Description
	processed. Select this option if your IdP is ADFS 2.0.
IdP SSO Service URL	Enter the URL to which Workday sends SAML authentication requests. You can get this URL from your SAML IdP.
Managed Device Attribute	Enter the name of the attribute that this IdP returns with its SAML assertion when the IdP is configured to return managed device status. When the **Device is Managed** check box is selected on an authentication policy, Workday checks the SAML assertion to determine if the value of this attribute is true. True indicates that the device the user is signing in from is a managed device. Any other value indicates that the device the user is signing in from isn't a managed device.
Used for Environments	(Optional) When you don't select an environment for the IdP, that IdP applies to any environment.
Preview Only	(Optional) Select to enable the IdP for preview tenants in the selected environments, except for the production environment.

6. As you complete the **SAML Setup** section, consider:

Option	Description
x509 Private Key Pair	(SP-Initiated SAML only) Select or create the X.509 private key pair that Workday uses to sign SAML sign-in requests. See Create an X.509 Private Key Pair. Required if you select the **Sign SP-initiated Request** check box. Provide the public key to your SAML provider.
Authentication Request Signature Method	Use *SHA256* as the method for signing authentication requests.
Enable Signature KeyInfo Validation	(Optional) Workday compares the optional SAML keyInfo element in incoming SAML messages with the stored SAML public key of your tenant. If the values don't match, Workday rejects the authentication request and records an error message on the **Signons and Attempted Signons** report. **Note:** The keyInfo element must contain the X.509 certificate that Workday uses to verify signed requests. It can't contain any other key management information, such as an IssuerSerial or path.
Additional Negative Skew (in minutes)	(Optional) The number of minutes to add to the NotBefore or NotOnOrAfter time when processing

Option	Description
Additional Positive Skew (in minutes)	the validity of a SAML assertion. Workday enforces a maximum of 3 minutes from the IssueInstant of the message to the current Workday server time. Skew is the difference between the Workday server time and your IdP server time.

7. In the **Single Sign-on** section, enter SAML redirect URLs in the **Redirection URLs** grid for each environment you're setting up. Redirect URLs must use HTTPS:

Option	Description
Redirect Type	The login and mobile login redirect URLs that Workday uses for SAML SSO. • **Single URL** uses a single authentication option for all users. This option uses the login redirect URLs configured in the **Redirection URLs** grid. • **Authentication Selector** uses the login redirect URLs configured on the selected authentication selector. Select this option when user groups from your organization use different authentication options to sign in. Workday builds a custom sign-in page for your tenant based on the authentication selector configuration.
Login Redirect URL	Enter the URL to which Workday redirect users for authentication. If you're using an authentication selector, configure this redirect URL on the authentication selector instead: (IdP-Initiated SAML) Typically the sign-in page for your IdP. (SP-Initiated SAML) https://<*workday host*>/<*tenant name*>/login-saml2.htmld.
Logout Redirect URL	Enter the URL to redirect users to when they click the **Sign Out** button (typically the sign-out page for your IdP).
Timeout Redirect URL	Enter the URL to redirect users to when their Workday session times out. Typically, this URL is the same as the **Logout Redirect URL**.
Environment	The Workday environment to which the URLs apply.
Preview Only	Select to enable the URLs for preview tenants only in the selected environment, except for the production environment.

Next Steps

Access the **Signons and Attempted Signons** report to monitor SAML authentication attempts during a specific time period.

Related Information
Concepts
Concept: Configuring Your SAML Provider on page 56
Concept: SAML Authentication on page 61
Reference
Reference: Edit Tenant Setup - Security

Configure SAML Single Logout

Prerequisites

- Configure Security Assertion Markup Language (SAML) authentication for your tenant.
- Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can enable your users to sign out of both the identity provider (IdP) and Workday with a single action, by configuring SAML single logout (SLO). We recommend you configure SLO if your IdP supports it. Without SLO, valid user sessions might still exist at the IdP or Workday after sign-out, enabling users to create a new Workday session without entering credentials. Workday supports these SLO flows:

- Workday-initiated logout: The user signs out of Workday, and Workday and the IdP exchange logout messages to end the user's IdP session.
- IdP-initiated logout: The user signs out at the IdP, and the IdP and Workday exchange logout messages to sign the user out of Workday.

Steps

1. Access the **Edit Tenant Setup - Security** task.
2. As you complete the **SAML Identity Providers** grid, consider:

Option	Description
Enable IdP-Initiated Logout	(Optional) You also need to configure the **Logout Response URL** and **x509 Private Key Pair**.
Logout Response URL	Enter the URL to which Workday sends a successful logout response message to the IdP. You can get this URL from your SAML IdP. If you imported a metadata XML file for the IdP, and the file includes this URL, Workday automatically completes this field.
Enable Workday Initiated Logout	(Optional) You also need to configure: • **Logout Request URL** • **Service Provider ID** • **x509 Private Key Pair**
Logout Request URL	Enter the URL to which Workday sends SAML logout request messages. You can get this URL from your IdP.
Service Provider ID	(Workday Initiated Logout only) Identifies Workday as the service provider in the Issuer element of SAML messages sent to the IdP.

Option	Description
x509 Private Key Pair	Select or create an X.509 private key pair that Workday uses to sign SAML sign-out requests.

3. Provide the public key portion of your selected X.509 private key pair to your IdP:
   a) Access the **View x509 Private Key Pair** report.
   b) Copy the entire contents of the **Public Key** field, including -----*BEGIN CERTIFICATE*----- and -----*END CERTIFICATE*-----.
   c) Provide the public key to your IdP.

Hide Password Management Tasks

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can hide these tasks from users who shouldn't use a password that Workday stores, such as those using delegated authentication or SAML authentication:

- **Change Password**
- **Manage Password Challenge Questions (Do Not Use)**

To hide the tasks from a group of users, modify the *Self-Service: Account* security domain policy to remove their permissions. The *All Users* security group automatically has access to this domain.

Steps

1. Run the **Domain Security Policies for Functional Area** report.
2. Select *System* from the **Functional Area** prompt.
3. Click the *Self-Service: Account* security domain, and then click **Edit Permissions**.
   You can add or remove security groups for the domain security policy.
4. Access the **Activate Pending Security Policy Changes** task to confirm changes.

Result

Only security groups belonging to the domain security policy can access the **Change Password** and **Manage Password Challenge Questions (Do Not Use)** tasks.

Create or Edit SAML SSO Links

Prerequisites

Configure these settings on the **Edit Tenant Setup - Security** task:

- **x509 Private Key Pair**, which Workday uses to sign the SAML Response sent to your SAML Identity Provider (IdP).
- **Service Provider ID**, which Workday uses as the default Issuer ID in all SAML SSO links.

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can create and edit SAML SSO links that use Workday as a SAML IdP to sign in to other systems from Workday. Depending on your link configuration, you can also pass contextual data to external systems. Workday supports both SAML 1.1 and SAML 2.0.

Steps

1. Access one of these tasks:
   - **Create SAML SSO Link**
   - **Edit SAML SSO Link**
2. Select a **SAML Version** the link is compliant with.

   For links that use SAML 2.0, you can also select the **Use unspecified Name ID format** check box. Selecting that check box causes the link to generate SAML 2.0 assertions containing a subject with the Unspecified Name ID format.
3. Enter the **Assertion Consumer Service URL** for the endpoint of the target system that receives the SAML assertion.
   Example: When Workday acts as a SAML endpoint, the **Assertion Consumer Service URL** ends with `../login-saml.htmld`.
4. Select a **Name Identifier** that the link uses to authenticate the account, through SAML, to the target system. You can select *Workday Identifier* to provide a static and unchangeable field that you can rely on for SAML authentication to other applications.
   If you select *Workday Identifier*, Workday uses the Workday Identifier for the requesting account in the SAML Name ID element in its SAML Response.
5. Select the **Signature Method** for the link.

   Workday requires *SHA256*.
6. Enter a **Recipient** URL. Your target service provider might specify this URL for you. This value is typically the same as the **Assertion Consumer Service URL**.
7. In the **Message Signing** list, select an option to sign the SAML message, the SAML assertion, or both the message and assertion.
8. As you complete the task, consider:

Option	Description
Audience	(Optional) A URL that your target service provider might specify.
Destination URI	(Optional) If the **SAML Version** for the link is *SAML 2.0*, the URL to which the sender has instructed the user agent to deliver the message. The Destination XML attribute in the root SAML element of the protocol message contains this URL. Then the recipient must verify that the value matches the location where the message was received.
Deeplink	(Optional) The URL to direct the user to after the authentication process is complete.
Issuer ID	(Optional) A unique identifier for this link, which overrides the **Service Provider ID** field on the **Edit Tenant Setup - Security** task (the default if not specified).
x509 Private Key pair	(Optional) Create or select a specific SAML X.509 key pair to use for this SAML SSO link instead of the key pair configured on the **Edit Tenant Setup - Security** task.

9. (Optional) Under **Additional Information**, select a **Condition Rule** for the link. This rule determines the users for which this link displays on any configured worklets and reports that filter on the **Valid for Worker** setting.

10. Configure the dynamic attributes for the link, which are name/value pairs that the service provider requires in the SAML assertion to validate it. Workday evaluates these dynamic attributes based on the processing user when a user clicks the SAML SSO link.
    a) Enter the **Attribute Name**.
    b) Enter a static **Attribute Value**.
    c) From the **Dynamic Attribute Value** prompt, select 1 of these dynamically obtained values for the attribute:
       - *Email Address*
       - *Employee ID*
       - *User Name*
       - *Workday Identifier*
11. Configure external fields for the link, which provide contextual data that the external system can process. Workday evaluates these links based on the processing user and the context when a user clicks the link. Workday only supports these links in certain business processes where a context is available for evaluation.
    Example: Configure a SAML SSO link for recruiters that signs them in to an external job posting site and populates the job posting page with details from Workday.
    a) From the **Business Object to Evaluate Fields for SAML attributes** prompt, select the Workday *business object* containing the report fields you want to include in the SAML SSO link.
    Example: To pass contextual data about a job, select *Job Profile* as the business object.
    If this link is currently in use, or has been removed from a To Do, you can't change this setting on the **Edit SAML SSO Link** task.
    b) Configure external fields for the SAML SSO link. Enter the **Attribute Name** and select the **Field** to use in the SAML SSO link. Workday restricts the available external fields to those fields associated with the selected business object.
    Example: Configure these external fields to pass to the job posting site to process and prepopulate the page:
       - ID
       - Job Description
       - Countries for Job Profile

Result

The SAML SSO link is available to use as an external link throughout Workday.

Note: If you configure a SAML SSO link incorrectly or use it in a location that provides insufficient context for evaluation, Workday displays an error message when users click the link.

You can access the **View SAML SSO Link** report to view details for it. You can't delete a SAML SSO link if it is in use.

Next Steps

Add the SAML SSO link to a:

- To Do step in a business process (**Maintain To Do** task).
- Navigation worklet or Quicklinks Group.

Related Information

Concepts

Concept: Integration IDs

Tasks

Steps: Display a Quicklinks Worklet on a Dashboard

Reference

Reference: Edit Tenant Setup - Security

Generate SAML Metadata

Context

Workday enables you to generate SAML metadata, so that SAML Service Providers that rely on Workday as a SAML Identity Provider for authentication can be easily configured.

Steps

From the related actions menu of a SAML SSO Link or Quicklink, select **SAML SSO Link** > **Generate Metadata**.

Result

This task returns the SAML metadata necessary for the configuration of a SAML Service Provider:

- SAML entity ID
- SAML public key
- URL (and the associated binding) to which unauthenticated user agents are sent

Steps: Decode and Validate a SAML Message

Context

You can decode SAML messages that Workday receives from the IdP so that you can view the structure, elements, and attributes of the SAML response.

IdPs secure SAML messages they send to Workday using Base64 type encoding. Workday stores the messages it receives in the encoded format. You must decode them to view them in readable XML format.

Steps

1. Access the **Signons and Attempted Signons** report and select the **Show Signon Attempts with an Invalid User Name** check box.

   Signon details display on both the **Signons** and **Signon Attempts with an Invalid User Name** tabs in the report.

   Security: These domains in the System functional area:

   - *Workday Account Monitoring*
   - *Workday Accounts*
2. Click the magnifying glass icon in the **Signon** column for the SAML sign-in or attempted sign-in record for which you want to view the SAML response.

   The page displays the SAML response as a base-64 encoded string labeled **User Credentials**.
3. Select and copy the entire contents of the **User Credentials** field.
4. Access the **Validate SAML Message** report.

   Security: *Security Administration* domain in the System functional area
5. Paste the contents of the **User Credentials** field into the **SAML Message** field, and select the **Is Message Base64 Encoded?** check box.

Result

Workday:

- Decodes the user credential information and displays the decoded SAML response in the **SAML Message** field.
- Displays the result of the validation in the **Validation Result** field.

Next Steps

Use the message Workday displays in the **Validation Result** field to troubleshoot possible SAML authentication issues. Example: No System Account for the UserName: vtaylor.

Related Information
Reference
Troubleshooting: SAML on page 62

Concept: Configuring Your SAML Provider

Before you can enable Security Assertion Markup Language (SAML) in Workday, you must configure your SAML identity provider (IdP) so that it passes the required information to Workday.

Note: To generate Service Provider metadata in XML format, access the **Generate Workday SAML Metadata** report. You can use the data generated with that report to configure your SAML provider.

Additionally, these requirements apply:

- Your IdP must use the SAML 2.0 HTTP POST binding.
- Workday doesn't support SAML encryption (name identifiers, attributes, or the assertion itself). However, you can configure Workday to sign SAML Requests it sends to your SAML IdP with your configured SAML public key. You can thus ensure the integrity of the SAML flow. The Destination XML attribute in the protocol message root element should contain the URL to which the sender has instructed the user agent to deliver the message. The recipient must then verify that the value matches the location at which it receives the message.

  Although incoming SAML messages to Workday must be signed, outgoing SAML messages (for Service Provider (SP)-initiated SAML) are optionally signed.
- The SAML request that Workday uses for step up authentication uses the Authentication Context Class Reference attribute that you configure. This attribute is also configured on the IdP and used as a mechanism to force user credentials at each authentication request within an existing IdP session. Workday also has the Force AuthN flag attribute set to True as another method for forcing credentials. Ensure that your IdP recognizes the Authentication Context Class Reference or the ForceAuthN=true flag for proper step up authentication operation.

SAML URLs

Depending on the SAML authentication flow that you use, consider these Workday SAML URLs that you need to configure SAML authentication for Workday:

URL	Description
`https://<workdayhost>/<tenantname>/login-saml.htmld`	(Both IdP-initiated and SP-initiated SAML) The URL where your IdP sends SAML response messages to Workday. • You need to provide this URL to your SAML IdP. • Users can't access this URL in their browser.
`https://<workdayhost>/<tenantname>/login-saml2.htmld`	(SP-initiated SAML) The URL to which the client of the user redirects them when they access Workday. • Use this URL as the **Login Redirect URL** when you configure SP-initiated SAML. • Users can access this URL in their browser.
`https://<workdayhost>/<tenantname>/login-saml.html`	(Both IdP-initiated and SP-initiated SAML) The Accessibility URL where your IdP sends SAML response messages to Workday.

URL	Description
	• You need to provide this URL to your SAML IdP. • Users can't access this URL in their browser. • Set this URL as the ACS URL on the IdP.

SAML Sign Out

When a user signs in to Workday using SAML, it maintains 2 sessions: One with Workday and 1 with the IdP. During sign out, Workday can handle these sessions in these ways:

- IdP-initiated sign out.
- Workday-initiated sign out.

In IdP-initiated sign out, Workday:

- Receives the SAML LogoutRequest message from an IdP.
- Signs the user out of the Workday session.
- Sends a SAML LogoutResponse message to the IdP.

In Workday-initiated sign out:

- Workday generates the SAML LogoutRequest message and sends it to the IdP.
- The IdP signs the user out of the SSO session and causes the Workday SAML session to end.
- Workday redirects the SAML LogoutResponse message.

You can configure how Workday handles sign outs with these settings on the **Edit Tenant Setup - Security** task:

- **Enable IdP Initiated Logout** for IdP-initiated sign out.
- **Enable Workday Initiated Logout** for Workday-initiated sign out.

If you don't enable either IdP- or Workday-initiated sign out, Workday:

- Ends the session when the user signs out.
- Doesn't send a SAML LogoutRequest or LogoutResponse message to the IdP.

The IdP session, if valid, will still exist and might enable a user to create a new Workday session without entering credentials.

For Workday-initiated sign out, your IdP must provide to you the URL where Workday will send the SAML LogoutRequest. You also need to provide a URL to the IdP so that the IdP can send SAML LogoutRequest and LogoutResponse messages to Workday. Use this format:

`https://<workdayhost>/<tenantname>/logout-saml.htmld`

Users can't access this URL in their browser.

Sample SAML Response and Required Elements

You can review this sample SAML response message that Workday expects from your IdP.

```
<?xml version="1.0" encoding="UTF-8"?>
<saml2p:Response xmlns:saml2p="urn:oasis:names:tc:SAML:2.0:protocol"
        ID="id254966580614828975952488885"
 InResponseTo="_031227df-127a-4902-9137-20a8dee72976"
        IssueInstant="2015-11-13T20:14:52.082Z" Version="2.0">
        <saml2:Issuer xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
          Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">kklfpz4sIWMADBSCWWIV</saml2:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
```



```
        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
        <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
        <ds:Reference URI="#id254966580614828975952488 85">
          <ds:Transforms>
              <ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature" />
              <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
          </ds:Transforms>
          <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#sha256" />
          <ds:DigestValue>NR6ebMcmjMEKDFnLwPZNtVfUficRBQnCNDFUx7xDBFo=</
ds:DigestValue>
          </ds:Reference>
          </ds:SignedInfo>

 <ds:SignatureValue>VyDP/5h6ashfnRSiTMENXGRTvU5SstYnQUJp7+aMp3MsufMZSBH8pMIukuYl9FQrmnN1
QBtDBTFxcxv0IUOPVpOu9IzDjcCKKCNWRVrkE+L3znK7n9D1eOnuXgNKreWvX
+xmYGTXejwJ3sEFuJDLlMDa/UYwrtVK+kO4=</ds:SignatureValue>
          <ds:KeyInfo>
          <ds:X509Data>
          <ds:X509Certificate>MIICxzCCAjCgAwIBAgIGASav/
CIVMA0GCSqGSIb3DQEBBQUAMIGmMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU
+Hh7iZCuIo5nhYUeDBhyqdjNFEYi9+hV8U/adh0PGpsBz5sLz+GpLom0KfTAqUVcg0x8yoIh
+naHFCoxI2enGlwGo+A7irCPlasEUbonhDVL6aUVIXFdZpg+QZ7gl1+ipjElykJ6fVkOVQ9Ur/
ZsRFqKzEdoJcZLjFlimTEsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQA11jpQqWz4tCzM/0vjve
+0V6rMqL63Jflto163GMfG+nXqxfyhfUce2oNDJ9UXFv4JosejJKjS9pnCTpuhTM/
A5t88DYyh8Pb6qIt1q/n9+b9iVV7aY9ni/+dsWrOLSFiZyAvL0cLnNrKf5a9msbtY
+Fw6BqM9+tIngcETJcm6pg==</ds:X509Certificate>
          </ds:X509Data>
          </ds:KeyInfo>
          </ds:Signature>
          <saml2p:Status>
        <saml2p:StatusCode
 Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
          </saml2p:Status>
        <saml2:Assertion xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion"
        ID="id254966580615618181601317 92"
 IssueInstant="2015-11-13T20:14:52.082Z"
          Version="2.0">
        <saml2:Issuer
          Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:entity">kklfpz4sIWMADBSCWWIV</saml2:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
          <ds:SignedInfo>
          <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/
xml-exc-c14n#" />
          <ds:SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
          <ds:Reference URI="#id254966580615618181601317 92">
              <ds:Transforms>
                <ds:Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature" />
                <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#" />
              </ds:Transforms>
              <ds:DigestMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#sha256" />
              <ds:DigestValue>3GW8REEVqrvATmoWfiYUJE0N2BFLNpDI/WgDfQb3qbE=</
ds:DigestValue>
          </ds:Reference>
          </ds:SignedInfo>
```



```
 <ds:SignatureValue>dSZkr8QhijRfUxbvd4EJU2JdHL4VUyJjH4nycPRoD37DVINz4dYzWq3CdgWaDaXNXZg
As1LBvJTxlkCP8z6iDT1TUouCSXabHNw7GPsJuap9NhyeQh8ISGzLPm3DL6d4pYMW/az
+RuuJNNSnuw=</ds:SignatureValue>
          <ds:KeyInfo>
          <ds:X509Data>
          <ds:X509Certificate>MIICxzCCAjCgAwIBAgIGASav/
CIVMA0GCSqGSIb3DQEBBQUAMIGmMQswCQYDVQQGEwJVUzETMBEGA1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU
+Hh7iZCuIo5nhYUeDBhyqdjNFEYi9+hV8U/adh0PGpsBz5sLz+GpLom0KfTAqUVcg0x8yoIh
+naHFCoxI2enGlwGo+A7irCPlasEUbonhDVL6aUVIXFdZpg+QZ7gl1+ipjElykJ6fVkOVQ9Ur/
ZsRFqKzEdoJcZLjFlimTEsCAwEAATANBgkqhkiG9w0BAQUFAAOBgQA11jpQqWz4tCzM/0vjve
+0V6rMqL63Jflto163GMfG+nXqxfyhfUce2oNDJ9UXFv4JosejJKjS9pnCTpuhTM/
A5t88DYyh8Pb6qIt1q/n9+b9iVV7aY9ni/+dsWrOLSFiZyAvL0cLnNrKf5a9msbtY
+Fw6BqM9+tIngcETJcm6pg==</ds:X509Certificate>
          </ds:X509Data>
          </ds:KeyInfo>
          </ds:Signature>
          <saml2:Subject>
        <saml2:NameID
          Format="urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified">lmcneil</saml2:NameID>
        <saml2:SubjectConfirmation
 Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
          <saml2:SubjectConfirmationData
 InResponseTo="_031227df-127a-4902-9137-20a8dee72976"
        NotOnOrAfter="2015-11-13T20:19:52.082Z" Recipient="https://
i-8054ce44.workdaysuv.com/super/login-saml.flex" />
          </saml2:SubjectConfirmation>
          </saml2:Subject>
        <saml2:Conditions NotBefore="2015-11-13T20:09:52.082Z"
          NotOnOrAfter="2015-11-13T20:19:52.082Z">
          <saml2:AudienceRestriction>
          <saml2:Audience>http://www.workday.com</saml2:Audience>
          </saml2:AudienceRestriction>
          </saml2:Conditions>
        <saml2:AuthnStatement AuthnInstant="2015-11-13T20:14:52.082Z"
          SessionIndex="_031227df-127a-4902-9137-20a8dee72976">
          <saml2:AuthnContext>

 <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTra
saml2:AuthnContextClassRef>
          </saml2:AuthnContext>
          </saml2:AuthnStatement>
          </saml2:Assertion>
</saml2p:Response>
```

Workday requires these elements in SAML response messages it receives from your IdP:

Element	Details
Issuer	The identity provider ID. The Issuer element must be present in both the SAML Response element and the SAML Assertion element.
Signature	Your SAML provider must sign the entire SAML message, not just the Assertion element.
Destination	The POST URL where the IdP sent the SAML message.
Subject	The NameID must match the Workday account ID.

Element	Details
Conditions	For the Workday production environment, set the Audience to: `http://www.workday.com` or start with: `http://www.workday.com/`. You can append to this value to enable your single SAML IdP to authenticate to multiple Workday environments. • Example: For the SANDBOX environment, set the Audience to: `http://www.workday.com/sandbox` or start the Audience with: `http://www.workday.com/sandbox/`. • Example: For the IMPL environment, set the Audience to: `http://www.workday.com/implementation` or start the Audience with: `http://www.workday.com/implementation/`.

Other Considerations
When you configure your SAML provider for signing in to Workday from other identity management providers, also consider:

Consideration	Description
SAML Assertion Consumer Service (ACS) URL	The URL where Workday receives SAML assertions: `https://<workdayhost>/<tenantname>/login-saml.htmld` This URL is identical to the default sign in page URL, except that the `login.htmld` target is replaced with `login-saml.htmld`.
Default RelayState URL	Redirects your users to their default Workday landing page: `https://<workdayhost>/<tenantname>/d/home.htmld`
SAML response validity range	Set to a maximum of +/- 3 minutes from the time that Workday receives the SAML response. You can specify a smaller range using the `Conditions:NotBefore` and `Conditions:NotOnOrAfter` elements.

Related Information
Tasks
Steps: Set Up Delegated Authentication on page 69
Steps: Set Up SAML Authentication on page 46
Reference
Reference: Edit Tenant Setup - Security
Workday Community: Finding your Workday Data Center using your Workday Tenant URL

Concept: SAML Authentication

You can use Security Assertion Markup Language (SAML) for Single Sign-On (SSO) and single logout (SLO) in Workday. SAML is a standard for exchanging authentication and authorization data between security domains, enabling you to manage user credentials centrally through a third-party identity provider (IdP). Example: A security administrator can disable a user account without directly signing in to Workday.

Workday supports the SAML 2.0 SSO standard for signing in to Workday from other identity providers.

How SAML Works

When you enable SAML authentication for signing in to Workday:

1. Your SAML IdP authenticates users and sends a SAML response message to Workday.
2. Workday either grants or denies access to a user based on the SAML assertion in the response message.

You can configure 2 types of flows in Workday based on who sends the first SAML message:

- In IdP-initiated SAML, the SAML provider sends an unsolicited SAML response message to Workday.
- In SP-initiated SAML, Workday sends a SAML authentication request message to your SAML provider.

When you enable SAML for signing out of Workday using your IdP, you can configure 2 flow types in Workday based on who sends the first SAML message:

- In IdP-initiated SLO, your SAML provider sends a SAML LogoutRequest message to Workday.
- In Workday-initiated SLO, Workday signs the user out of Workday and sends a SAML LogoutRequest message to your IdP.

During the SAML authentication process, all SAML messages must:

- Pass through the user's browser or mobile client. Workday doesn't support SAML Artifacts.
- Use HTTPS.
- Be signed by the IdP if they’re incoming to Workday.

Redirect URLs

SAML redirect URLs enable the integration of SAML with Workday. Specify redirect URLs as alternative URLs to reference when users make unauthenticated requests to Workday. These redirect URLs:

- Apply to the Workday sign-in page, the Workday **Sign Out** button, and deeplinks that reference Workday authentication URLs.
- Must use HTTPS.
- Apply to all users.

To avoid continuous loops when the IdP session is still active, use different URLs for the **Login Redirect URL** and **Logout Redirect URL**. If you're not using SLO, signing out of Workday doesn't end a user's IdP session, possibly enabling the user to access Workday again without authenticating.

Deeplinks

Don't use deeplinks that use query string parameters (Example: returnTo) to try to link to resources within Workday (Example: A learning course). Use simple URLs that directly reference the resources instead.

If you want to use such deeplinks and you set up your tenant to use SAML SSO, use:

- An authentication selector if your tenant configuration uses multiple forms of authentication. Example: Some users sign in using different SAML IdPs and others sign in using user name password authentication.
- Redirection URLs in the tenant configuration if all users use the same SAML IdP.

Workday doesn't use the RelayState parameter in outbound authentication requests. When Workday receives an authentication request from a user accessing a deeplink, it stores a cookie containing the

deeplink during SSO redirects for both IdP-initiated and SP-initiated SAML. When Workday receives responses to authentication requests, it navigates to the deeplink it stored. If Workday hasn't stored a deeplink during an SSO redirect, it navigates to the:

- Inbound RelayState setting, if the response contains one.
- Workday Home page, if the response doesn't contain an inbound RelayState.

X.509 and SAML

Workday SAML features require that you use X.509 certificates to sign SAML messages.

Create an X.509 public key in Workday to verify the digital signature on incoming SAML sign-in and sign-out requests. Your IdP must use a corresponding X.509 private key to sign those files.

To configure Workday to participate in SAML sign-out transactions, create an X.509 private key pair in Workday, and ensure that the public key is available to your IdP. When Workday generates SAML sign-out request and sign-out response messages, it uses the X.509 private key to sign the messages. Your IdP uses the corresponding X.509 public key to verify that the SAML sign-out requests and responses came from your Workday tenant. Public keys must be in PEM format.

Related Information
Tasks
Steps: Set Up SAML Authentication on page 46

Troubleshooting: SAML

This topic provides strategies for diagnosing and resolving these SAML issues:

- Workday displays a sign in error - SP-initiated SAML. on page 62
- Workday displays a sign in error - other conditions. on page 63
- No or incorrect redirect during SP-initiated SAML. on page 66
- Incorrect IdP sign-in page displays, or Workday unable to connect to the IdP server. on page 67
- IdP server returns a page not found error. on page 67
- SAML POST returns a server error on all sign-in attempts. on page 67
- Browser hangs on a SAML POST or seems to refresh continuously. on page 68
- No SSO access to the Sandbox Preview tenant after the start of the release preparation window. on page 68
- SAML Single Logout (SLO) Fails With No Apparent Indication.

Note: You might need to bypass SAML and sign in to your tenant using Workday user name password authentication to troubleshoot SAML issues. If your tenant doesn't have an authentication policy in place to enable administrators to bypass SAML (Example: An authentication rule that enables administrators to sign in using **User Name Password** authentication), use this URL. Don't share it with your users: `https://<workdayhost>/<tenantname>/login.htmld?redirect=n`.

Workday displays a sign in error - SP-initiated SAML.

When users attempt to sign in using SP-initiated SAML, the browser displays **Workday Sign In Error**. It also displays a message that indicates that the tenant isn't configured for SP-initiated SAML authentication.

Solution:

Steps

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

1. Access the **Edit Tenant Setup - Security** task.
2. Select the **SP Initiated** check box and populate the **Service Provider ID** field.

Workday displays a sign in error - other conditions.

When users attempt to sign in with SAML, the browser displays **Workday Sign In Error** and a message that indicates 1 of these conditions:

- The user entered an invalid user name or password.
- The system is restricting new sessions.

Cause: Many different issues might cause Workday to display a **Workday Sign In Error**. The **Signons and Attempted Signons** report can provide more insight into the cause.

Solution:

Steps

1. Access the **Signons and Attempted Signons** report, and select the **Show Signon Attempts with an Invalid User Name** check box.

   Security: These domains in the System functional area:

   - *Workday Account Monitoring*
   - *Workday Accounts*
2. Search the report for records where:
   - **Authentication Type for Signon** is SAML.
   - **Failed Signon** is Yes.
   - **Authentication Failure Message** is populated.
3. Match the failure message displayed in the report with the solution in this table.

Authentication Failure Message	Solution
Audience value does not match the required value, 'http://www.workday.com.'	Ensure that the IdP has the Audience set to http://www.workday.com/<*tenant name*>, where <*tenant name*> is optional.
Current date is before SAML assertion's NotBefore date.	Perform these actions as necessary to resolve the issue, in the order suggested: • Resynch the time on the IdP with the time on the Workday server, if the difference falls outside the skew times defined in the IdP. • Ensure that the NotBefore condition set at the IdP isn't greater than -3 minutes. • Set a skew of up to -3 minutes on the IdP for the NotBefore condition. Some IdPs automatically set this skew to zero. • Select an **Additional Negative Skew (in minutes)** on the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area.
Current date is equal to or after SAML assertion's NotOnOrAfter date.	Perform these actions as necessary to resolve the issue, in the order suggested: • Resynch the time on the IdP with the time on the Workday server, if the difference falls outside the skew times defined in the IdP. • Ensure that the NotOnOrAfter condition set at the IdP isn't greater than +3 minutes.

Authentication Failure Message	Solution
	• Set a skew of up to +3 minutes on the IdP for the NotOnOrAfter condition. • Select an **Additional Positive Skew (in minutes)** on the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area.
Issuer value does not match the value specified in Tenant Setup - Security.	**1.** Access the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area. **2.** Ensure that the **Issuer** value matches the SAML Issuer value defined in your IdP.
No Identity providers are enabled or selected for this environment for the SAML Issuer.	**1.** Access the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area. **2.** Clear the **Disabled** check box for the IdP, if selected. **3.** Ensure that the value in the **Issuer** field is correct. **4.** Ensure that the **Used for Environments** field is set correctly.
SAML X.509 certificate is not yet valid, current date is before X.509 certificate's Valid From date. X.509 certificate is expired, current date is after X.509 certificate's Valid To date.	**1.** Access the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area. **2.** Check if the **x509 Certificate** selected for the IdP has a: • *Valid From* date that occurs before the current date. • *Valid To* date that occurs after the current date. Free third-party tools are available that you can use to verify X.509 certificate dates. Example: Portecle. **3.** If either or both conditions are true, then replace the **x509 Certificate** with an updated valid certificate from the IdP. See Create an X.509 Public Key on page 223.
Signature cannot be verified using any of the X.509 certificates specified in Tenant Setup - Security.	**1.** Access the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Authentication Failure Message	Solution
	2. Ensure that the **x509 Certificate** selected for the IdP: • Matches the X.509 public key provided by your IdP. • Is PEM encoded and has no extra characters, spaces, or line feeds. 3. Correct any issues that you find with the certificate.
Signature is missing or does not refer to the entire message.	1. Ensure that the IdP signs the SAML response message, and that it signs the entire SAML message, not just the assertion. 2. If necessary, obtain an updated public key from the IdP, save it in Workday, and select it on **Edit Tenant Setup - Security** for the IdP. See Create an X.509 Public Key on page 223. Security: *Set Up: Tenant Setup - Security* domain in the System functional area.
Subject is missing.	Check the IdP configuration to ensure it passes the Subject element and NameID child element in the SAML response.
System Account locked out. System Account disabled.	If Workday locked the account or disabled it needlessly, access: • **Manage Workday Accounts** to unlock the account. See Lock and Unlock Workday Accounts on page 258. • **Edit Workday Account** to re-enable the account. See Edit Workday Accounts on page 246.
Tenant is not SAML enabled.	1. Access the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area. 2. Select the **Enable SAML Authentication** check box.
The SAML token is invalid. The current moment is after the time skew range of the issue date.	Ensure that the NotBefore and NotOnOrAfter conditions set at the IdP aren't greater than 3 minutes.
The system is temporarily restricting new sessions. Please try again later.	Security: *Security Administration* domain in the System functional area. 1. Access the **View Workday Maintenance Window History** report to see if a session restriction is in progress. 2. Access the **Manage Workday Maintenance Window** task to remove the session restriction if it isn't necessary.

Authentication Failure Message	Solution
	Tenants are also unavailable during the: • Weekly service update. • Workday maintenance window. The condition clears once the service update or maintenance window transpires.
Unable to decode X.509 certificate specified in Tenant Setup - Security.	1. Access the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area. 2. Ensure that the **x509 Certificate** selected for the IdP: • Matches the X.509 public key provided by your IdP. • Is PEM encoded and has no extra characters, spaces, or line feeds. 3. Correct any issues that you find with the certificate.

The browser displays **Workday Sign In Error** with a message indicating the user entered an invalid user name or password. You don't find an **Authentication Failure Message** in the **Signons and Attempted Signons** report, however.

Solution:

Steps

1. Access the **Signons and Attempted Signons** report, and select the **Show Signon Attempts with an Invalid User Name** check box.

   Security: These domains in the System functional area:

   - *Workday Account Monitoring*
   - *Workday Accounts*
2. If the **Invalid for Authentication Policy** field is populated for a SAML sign-in record, check the authentication policy. Ensure that the authentication rule against which Workday validated the sign-in has **SAML** as an **Allowed Authentication Type**.
3. Select **Signon Attempts with an Invalid User Name**.
4. If the **Invalid User Name** field is populated for a SAML sign-in record, ensure that the user's account information is synchronized between the IdP and Workday.

   Workday expects the user name passed from the SAML provider to match the value specified in the user name field in the Workday Account.

No or incorrect redirect during SP-initiated SAML.

When you've configured the Workday tenant for SP-initiated SAML Single Sign-On (SSO) and certain users attempt to sign in using the SP-initiated flow, SSO doesn't succeed. The browser also displays either:

- The Workday sign-in page.
- A message indicating that they can't reach the site.

Cause: Workday uses information from a browser's User Agent HTTP header to determine which redirect URL to use during SP-initiated SAML. Some user devices resemble laptop computers but contain mobile-like features, such as a touchscreen. The browser's user agent string might identify these devices as

mobile devices rather than laptop computers. In such cases, if the mobile browser redirect URL configured in Workday is missing or incorrect, SP-initiated SAML SSO fails.

Note: You can use certain online tools to parse and view a browser's user agent string. Example: WhatIsMyBrowser.

Solution:

Steps

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

1. Access the **Edit Tenant Setup - Security** task.
2. Ensure that the **Mobile Browser Login Redirect URL** field is populated and correct.

   You can:

   - Correct the **Mobile Browser Login Redirect URL** if it's incorrect.
   - Set the **Mobile Browser Login Redirect URL** to the same value as the **Login Redirect URL**.
   - Use an authentication selector with choices to sign in depending on what your users want to access. See Set Up Authentication Selectors.

Incorrect IdP sign-in page displays, or Workday unable to connect to the IdP server.

Solution:

Steps

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

1. Access the **Edit Tenant Setup - Security** task.
2. Ensure that the **Logout Redirect URL** is correct.
3. If the condition happens when users attempt to sign in to Workday using SP-initiated SAML, ensure that the **Login Redirect URL** is correct.

IdP server returns a page not found error.

The IdP server returns an HTTP 404 client error response when users attempt to sign in to Workday using SP-initiated SAML.

Solution:

Steps

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

1. Access the **Edit Tenant Setup - Security** task.
2. Ensure that the **IdP SSO Service URL** is correct.

SAML POST returns a server error on all sign-in attempts.

Cause: This problem might occur when you:

- Have a custom sign-in page that performs a POST to `https://<workdayhost>/<tenantname>/login-saml.x.`
- Receive the error message *Invalid request, should be POST*.

- Are unable to sign in on any subsequent attempts.

Solution: Verify that you've included a *RelayState* parameter in the original post along with the *SAMLResponse* parameter. If you want users to:

Steps

- View the Workday default landing page after successfully signing in, update the *RelayState* parameter value in the IdP to `https://<workdayhost>/<tenantname>/d/home.htmld`.
- View a specific Workday task or report after successfully signing in, specify the URL of the task. Example: To direct users to the My Payslips report, specify `https://<workdayhost>/<tenantname>/d/task/2997$1475.htmld` as the IdP *RelayState* parameter.

  Note: In the SAML 2.0 specification, the *RelayState* parameter specifies the destination URL (typically a deep link) of the user after signing in.

  Workday supports deep links that use either the *RelayState* parameter or the *Done* parameter for the username and password POST target (`https://<workdayhost>/<tenantname>/login-auth.htmld`) and the SAML POST target (`https://<workdayhost>/<tenantname>/login-saml.htmld`).

  If the POST request includes both *Done* and *RelayState* parameters, Workday redirects to the URL in the *RelayState* parameter and ignores the *Done* parameter.

Browser hangs on a SAML POST or seems to refresh continuously.

Solution: Check if a *RelayState* parameter is set at the IdP to `https://<workdayhost>/<tenantname>/login.htmld`. If it is, configure the IdP to change the *RelayState* parameter value to `https://<workdayhost>/<tenantname>/d/home.htmld`.

No SSO access to the Sandbox Preview tenant after the start of the release preparation window.

Cause: At the start of the release preparation window, Workday automatically refreshes your Sandbox Preview tenant from Production. After that refresh takes place, the Sandbox Preview tenant won't redirect correctly during SSO sign-in attempts if your Production tenant:

- Doesn't have redirection URLs configured for the Sandbox environment.
- Has redirection URLs configured for the Sandbox environment, but you haven't selected the **Preview Only** check box for that environment.

Solution:

Steps

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

1. Access the **Edit Tenant Setup - Security** task on your Sandbox Preview tenant.
2. Ensure that the redirection URLs are correct for the Sandbox Preview environment. Example: `https://<workdayhost>/sboxAcme_preview/login-saml2.htmld`, not `https://<workdayhost>/sboxAcme/login-saml2.htmld`.
3. Ensure that you've selected the **Preview Only** check box.

SAML Single Logout (SLO) Fails With No Apparent Indication.

When Workday is configured for Workday-initiated single logout and a user signs out from Workday:

- Workday signs out of the service provider (Workday), but doesn't sign out of the identity provider (IdP).
- The IdP responds with an HTTP OK response (200 response code).
- The user sees no indication in the Workday UI that the single logout operation didn't complete successfully.

Cause: The **Service Provider ID** is missing from the Workday-initiated single logout configuration for the tenant.

Solution:

Steps

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

1. Access the **Edit Tenant Setup - Security** task on the tenant.
2. In the row of the **SAML Identity Providers** grid for the identity provider being used for Workday-initiated single logout, populate the **Service Provider ID** field.

   The **Enable Workday Initiated Logout** check box is selected in the row that's configured for Workday-initiated single logout.

Related Information
Tasks
Steps: Decode and Validate a SAML Message on page 55
Examples
Example: Alternate Sign-In Option for OfficeConnect
Example: Emergency Sign-In for Administrators on page 89

Delegated Authentication

Steps: Set Up Delegated Authentication

Context

Note: Workday plans to retire delegated authentication in a future release. We recommend that you use other forms of authentication that we support.

You can integrate Workday with an identity-management system of your choice. Example: The identity-management system already in use by your organization. Workday then delegates tasks such as directory and authentication management to that identity management system.

By default, Workday uses its own directory and authentication management. When you use delegated authentication, your users enter their credentials on the Workday sign-in page, but the delegated authentication system manages those credentials.

Incorporating Workday into a delegated authentication system enables you to:

- Centrally manage identities. Example: A security officer can disable a user account without having to sign in to Workday.
- Use Single Sign-On (SSO).

You can use delegated authentication and Security Assertion Markup Language (SAML) authentication simultaneously for SSO.

Steps

1. Create a custom delegated authentication web service that Workday can call to verify the user name and password.

   See Concept: Delegated Authentication Web Service Guidelines.
2. Create a Configuration for Delegated Authentication on page 70.
3. Enable Delegated Authentication on page 70.
4. (Optional) Hide Password Management Tasks on page 71

Next Steps

Access the **Signons and Attempted Signons** report to review sign-ins through delegated authentication and SAML systems during a specified time period. Workday displays *Delegated Authentication* in the **Authentication Type for Signon** column of the report for sign-ins through delegated authentication.

Create a Configuration for Delegated Authentication

Context

Note: Workday plans to retire delegated authentication in a future release. We recommend that you use other forms of authentication that we support.

You can create a configuration to enable Workday to use a custom delegated authentication web service for password verification. You can configure one or more web service endpoints in the configuration, and optionally restrict the endpoints to specific Workday environments.

Create more than 1 configuration if you want to use separate delegated authentication systems for different users.

Example: You can have 1 system for employees and another for partners.

Steps

1. Access the **Create Delegated Authentication Configuration** task.
2. As you complete the task, consider:

Option	Description
Endpoint URL	The delegated authentication web service endpoint URL.
Restricted to Environment	(Optional) The target environment for the endpoint.

Only 1 endpoint URL is valid per environment, but you can add a row to the grid for each of your environments. You can also optionally add a row with a blank **Restricted to Environment** field for remaining environments. Example: You can add 2 rows for the production and implementation environments, and then add a third row with no selected environment to apply to all other environments.

Result

You can now enable delegated authentication for all users or for specific individuals.

Enable Delegated Authentication

Prerequisites

Note: Workday plans to retire delegated authentication in a future release. We recommend that you use other forms of authentication that we support.

- Ensure that Workday synchronizes with the user names in your third-party identity management system. Workday typically performs synchronization during implementation. Contact your engagement manager or implementation consultant for assistance.
- Create a configuration for delegated authentication.

Context

You can enable delegated authentication for all users or individual users. Workday lists each delegated authentication configuration as an option in the **Default Delegated Authentication System (Do Not Use)** field on the **Edit Tenant Setup - Security** task.

Workday strongly recommends that you exempt at least 2 Security Administrator users from delegated authentication using the **Edit Workday Account** task. If your delegated authentication system goes offline, your security administrator can sign in with a type of Workday-managed authentication. Example: User name password authentication. The security administrator can then exempt high-priority users (such as payroll administrators) from delegated authentication. Those users can then continue some high-priority operations while waiting for your delegated authentication system to become operational.

Note: A Security Administrator can change the password of a user to unlock an account that Workday has locked out due to multiple failed sign-in attempts. However, if you use delegated authentication, you must have the password reset in the delegated authentication system, not in Workday, to update Active Directory or LDAP account credentials.

Steps

1. Access the **Edit Tenant Setup - Security** task.
2. Under **Single Sign-On**, select the **Default Delegated Authentication System (Do Not Use)**. You created this configuration for custom delegated authentication.
3. Select the **Delegated Authentication Timeout (Do Not Use)**. The delegated authentication timeout is the length of time that Workday waits for a response from an external web service.
4. (Optional) Access the **Edit Workday Account** task for certain users.
   - Select the **Exempt from Delegated Authentication (Do Not Use)** check box to exempt the user from using your delegated authentication system. The user must then sign in directly to Workday.
   - Select a delegated authentication system to enable in the **Override Delegated Authentication Integration System (Do Not Use)** prompt. This selection overrides the delegated authentication system configured on the **Edit Tenant Setup - Security** task. This selection doesn't override the **Exempt from Delegated Authentication (Do Not Use)** check box.

Hide Password Management Tasks

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can hide these tasks from users who shouldn't use a password that Workday stores, such as those using delegated authentication or SAML authentication:

- **Change Password**
- **Manage Password Challenge Questions (Do Not Use)**

To hide the tasks from a group of users, modify the *Self-Service: Account* security domain policy to remove their permissions. The *All Users* security group automatically has access to this domain.

Steps

1. Run the **Domain Security Policies for Functional Area** report.
2. Select *System* from the **Functional Area** prompt.
3. Click the *Self-Service: Account* security domain, and then click **Edit Permissions**.
   You can add or remove security groups for the domain security policy.
4. Access the **Activate Pending Security Policy Changes** task to confirm changes.

Result

Only security groups belonging to the domain security policy can access the **Change Password** and **Manage Password Challenge Questions (Do Not Use)** tasks.

Concept: Delegated Authentication Web Service Guidelines

Note: Workday plans to retire delegated authentication in a future release. We recommend that you use other forms of authentication that we support.

Before you configure delegated authentication in Workday, follow these guidelines to create a custom delegated authentication web service.

Use Workday WSDL.	Ensure that you properly configure your custom delegated authentication web service. Create the web service using the Workday WSDL sample that we provide.
Unescape XML-Reserved Characters.	Workday escapes XML-reserved characters (" ' < > &) when passing the user name and password to your delegated authentication web service. Your web service must unescape these characters in the Workday message before authenticating the user account. Example: If you implement your web service in Java, you can use the Apache Commons Language StringEscapeUtils API.
Test Your Web Service.	Workday recommends that you run thorough performance and load tests on your custom delegated authentication web service. As part of this process, ensure that: • The server you deploy the web service on has enough capacity to support the expected amount of Workday sign-in attempts. • The identity management system can support the additional load due to Workday sign-in requests. • Testing involves enough users to match the number of open connections that you expect in production.
Check the Web Service Response Time.	To optimize Workday performance, Workday uses a 3-second timeout for delegated authentication sign-in attempts. If you receive a timeout exception error, verify that your custom delegated response time is 3 seconds or less. Alternatively, you can increase the **Delegated Authentication Timeout (Do Not Use)** value on the **Edit Tenant Setup - Security** task. Timeout values can be 1 to 15 seconds. Example: When a user initiates a sign-in attempt, the sequence of server connections in the delegated authentication flow is from the: **1.** Workday user interface to the Workday Object Management Server.

2. Workday Object Management Server to the Workday authentication framework.
3. Workday authentication framework to the delegated authentication web service endpoint in your environment.
4. Delegated authentication web service endpoint to your third-party identity management system.

The call response time from the Workday authentication framework must be:

- Under the selected timeout value.
- Under 3 seconds.

Workday can track the number of authentication timeouts and the response time of your delegated authentication web service. Log a support case to request a report from Workday Production Support.

Related Information
Reference
Supported Outbound SSL CA Certificates
Workday WSDL sample

OpenID Connect

Enable OpenID Connect Authentication

Prerequisites

- Client ID and client secret set for your Workday application with your OpenID Connect provider.
- Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can enable OpenID Connect for your tenant so that your OIDC provider can validate user credentials.

Steps

1. Access the **Edit Tenant Setup - Security** task.
2. In the **OpenID Connect Setup** section, select the **Enable OpenID Connect Authentication** check box.
3. Create the **OpenID Connect Provider**. Currently, Workday only supports Google as an OIDC provider.
   a. Enter a **Provider Name**.
   b. Enter the **Client ID**.
   c. Enter the **Client Secret**.
   d. Click **OK**.
4. (Optional) In the **Max OpenID Connect Session Age** field, enter a number between 1 and 60. This number is the maximum OpenID Connect session age in minutes before your OIDC provider requires users to reauthenticate.

   Note: Workday supports this feature only if your service provider supports it. As an OIDC provider, Google doesn't support this feature.

5. On the **Redirection URLs** grid in the **Single Sign-on** section, add a row and enter this URL as the **Login Redirect URL**:

   `https://host/tenant/login-init.htmld?authType=oidc`

Next Steps

Update your authentication policy to use OpenID Connect authentication for certain user populations (**Manage Authentication Policies** report). Workday recommends that you use multifactor authentication with OpenID Connect authentication if applicable.

Concept: OpenID Connect

Workday supports OpenID Connect (OIDC) authentication. You can configure it for your tenant and use it in your authentication policies, enabling your OIDC provider to validate user credentials for accessing Workday. Currently, Workday supports only Google as an OIDC provider.

Workday maps OIDC accounts to their associated Workday accounts based on email address using the **OpenID Identifier** field on a Workday account (**Edit Workday Account** task).

If your OIDC provider supports it, you can also configure OIDC for your tenant so that users must re-authenticate with their OIDC credentials after a certain period of time, even if they have an existing session with the OIDC provider.

When a user accesses Workday using OIDC:

1. Workday sends an authentication request to the OIDC provider.
2. The OIDC provider authenticates the user and sends an authentication response with an authorization code.
3. Workday sends the authorization code to the Token Endpoint to exchange it for an ID Token and an Access Token.
4. Workday receives a response that contains an ID Token and Access Token in the response body.
5. Workday validates the ID Token and retrieves the sub value for the user (**OpenID Connect Internal Identifier**).

The endpoint URL for signing in to Workday using OIDC is:

`https://host/tenant/login-init.htmld?authType=oidc`

When you configure OpenID Connect for your tenant, use this URL as your **Login Redirect URL**.

Troubleshoot: OpenID Connect Authentication

Access the **Signons and Attempted Signons** report to monitor and troubleshoot OpenID Connect (OIDC) authentication attempts. You can:

- Review failure messages in the report.
- Review the raw OpenID Connect token message.

Review Authentication Failure Messages

A % represents a string substitution with the state of the request being processed or a tenant configuration.

Authentication Failure Message	Description
OpenID Connect is not enabled in Tenant Setup Security.	OpenID Connect isn't configured on the **Edit Tenant Setup - Security** task.
Internal Processing Error parsing return from OpenID Connect Provider.	Workday couldn't parse the response from the OIDC provider.

Authentication Failure Message	Description
Failure reported from OpenID Connect Token Endpoint: %s - %s.	Workday received an error from the OpenID Connect Token Endpoint.
General Error: Failed to exchange auth code for id token.	Workday couldn't exchange the Authorization Code for an ID Token.
General Error: Failed to contact certificate endpoint for cert lookup.	Workday couldn't connect to the certificate endpoint. Example: SSL error or timeout.
No error reported from OpenID Connect Token Endpoint, but + ID_TOKEN_JSON_ATTR + was not present in response.	A particular ID Token JSON attribute was missing in the response.
General Error: Failed to contact OpenID Connect Token Endpoint - %s.	Workday couldn't connect to the OpenID Connect Token Endpoint.
General Error: Failed to contact OpenID Connect Certificate Lookup Endpoint - %s.	Workday couldn't contact the OIDC provider for successful certificate lookup.
Id Token signature validation failed	Workday couldn't verify the signature of the ID Token.
Audience: %s does not match registered client id: %s.	The audience value doesn't match the client_id.
OpenID Connect provider did not return email attribute in Id Token.	The OpenID Connect provider didn't send back an email address as part of the Id token claims.
OpenID Connect Issuer: %s does not match expected value: %s.	The Issuer Identifier for the OpenID Provider doesn't match the value of the issuer Claim.
OpenID Connect Id Token timing error: %s.	Invalid time range in Id Token.
Could not find Workday Account for OpenID Connect email: %s or subject: %s.	A Workday account wasn't found for the OIDC email address or OpenID Connect Identifier.
%s has internal user. OpenID Connect authentication is not allowed for internal users.	Workday doesn't enable internal users to sign in using OIDC.
No certificate found for kid: %s but did find: %s.	Workday couldn't locate the certificate for the key id.
Failed to convert and extract Public Key from Certificate: %s.	Workday couldn't extract the public key from the certificate.
User already mapped with different subject: %s vs. token subject of %s.	The user is already mapped to an **OpenID Connect Internal Identifier**.
Auth time in token %s is beyond configured max age of session %s seconds.	The time when the end-user authentication occurred is beyond the allowable elapsed time in seconds since the last time the end user was actively authenticated.
General Error trying to validate Auth time - %s.	Workday couldn't validate the authentication time for reauthentication.
OpenID Connect provider did not return auth_time in Id Token, though you specified a max session age.	**Max OpenID Connect Session Age** is set on the **Edit Tenant Setup - Security** task, but the OIDC provider didn't return auth_time in the ID Token.

Authentication Failure Message	Description
Token is too old, rejecting because it was generated more than 10 minutes ago.	The ID Token returned by the OIDC provider was generated more than 10 minutes ago and considered expired.
Invalid Hmac for timestamp, did not match expected value.	The hmac is no longer valid.
Failure reported from OpenID Connect Token Endpoint: internal_failure.	The OIDC provider had a problem with or failed to process the Auth code sent in exchange for the ID Token. Requires error processing by the OIDC provider.

Review the OpenID Connect Token Message

You can review the raw OpenID Connect token message available in the **Signon and Attempted Signons Report** to investigate further. Locate the base-64 encoded OpenID Connect token message in the **User Credentials** field when you view details for sign-in attempts.

OAuth

Register API Clients

Prerequisites

Security: These domains in the System functional area:

- *Set Up: Tenant Setup - Security*
- *Security Administration*

Context

Workday supports OAuth 2.0 as part of the Workday API Infrastructure. OAuth 2.0 enables Workday users to authorize third-party clients to access their Workday data securely on their behalf.

To access the Workday API, register OAuth 2.0 clients with Workday. You can enable OAuth 2.0 clients to access the Workday API for each tenant.

Steps

1. Access the **Edit Tenant Setup - Security** task.
2. In the **OAuth 2.0 Settings** section, select the **OAuth 2.0 Clients Enabled** check box.
3. Access the **Register API Client** task.
4. Enter the **Client Name**.
5. Select the **Client Grant Type**.

Option	Description
Authorization Code Grant	Use for clients that can persist data, such as mobile applications.
Implicit Grant (Do Not Use)	Necessary for applications that don't include a server-side component, such as JavaScript applications.

Option	Description
	Note: Workday plans to retire this client grant type in a future release. We recommend that you use these client grant types instead: • Authorization Code Grant with PKCE support. • JWT Bearer Grant.
JWT Bearer Grant	Use the JSON Web Token (JWT) for clients such as your Salesforce integration. This grant type enables you to restrict the exchange of security assertions for access and refresh tokens to Integration System Users (ISUs) you select in the **Integration System User** field. Provide an **x509 Certificate** for validating signatures. You can also select the **Allow Integration Messages** check box to ensure that Workday receives necessary information about the status of the integration.
SAML Bearer Grant	Use for applications that use SAML SSO for authentication. Also select an **Assertion Verification**. Select: • **Use Configured IdPs** to use the X.509 public certificate of the SAML IdP configured on **Edit Tenant Setup - Security** for validating signatures. The issuer in this case is the IdP. • **Use Certificate (x509 option)** to specify an **x509 Certificate** for validating signatures. The issuer in this case is the API Client ID. You can also optionally select ISUs in the **Integration System User** field, to restrict the exchange of security assertions for access and refresh tokens to those ISUs. You can also: • Select the **Allow Access to All System Users** check box to enable all users, rather than just Integration System Users (ISUs), to use the SAML bearer assertion flow. • Select the **Allow Integration Messages** check box to ensure that Workday receives necessary information about the status of the integration.

6. (Optional) Select the **Support Proof Key for Code Exchange (PKCE)** check box when using the **Authorization Code Grant** client grant type to add PKCE support to your client.

   PKCE enables the client to mitigate the threat of having the authorization code intercepted. Select this check box if the client will be supporting Cross Origin Resource Sharing (CORS)-enabled cross-origin requests.

7. (Optional) Select the **Enforce 60 Minute Access Token Expiry** check box to enable the API client to return bearer tokens that:
   - Have a 60-minute expiry.
   - Don't invalidate when sessions end, as long as they haven't expired.

   Once you select this check box and click **OK**, you can't clear it.
8. Select an X.509 public key in the **x509 Certificate** field.

   This field is active when you select:
   - **Jwt Bearer Grant** as the **Client Grant Type**.
   - **SAML Bearer Grant** as the **Client Grant Type** and **Use Certificate (x509 option)** as the **Assertion Verification**.
9. (Optional) Select 1 or more ISUs in the **Integration System User** field.

   This field displays when the **x509 Certificate** field is active. If you don't select any ISUs in this field, the API client won't restrict access based on ISU user accounts. If you select 1 or more ISUs, sign-in attempts using other users will fail. Workday recommends that you restrict the access of the client to specific ISUs.
10. Select the **Access Token Type**.

Option	Description
Bearer	Enables simpler development.
MAC (Do Not Use)	Provides increased security. **Note:** Workday plans to retire this access token type in a future release. We recommend that you use bearer tokens instead.

11. Enter the **Redirection URI**.
    - Use a comma as the delimiter to specify more than 1 redirection URI.
    - For **Authorization Code Grant** client grant types, only secure URIs starting with https are valid.
    - For **Implicit Grant** and **Authorization Code Grant** with **Proof Key for Code Exchange (PKCE)** enabled, only secure URIs starting with https and custom domain URIs are valid. Example: officeconnect://test.com and https://google.com.
12. (Optional) Select the **Refresh Token Timeout (in days)**. You can select a value between 1 and 365 days. The default value is 30 days.
13. (Optional) Select the **Non-Expiring Refresh Tokens** check box to prevent the refresh token from timing out.
14. (Optional) Select the **Disabled** check box to prevent the client from requesting access to Workday.
15. Select the **Grant Administrative Consent** check box when you want to grant OAuth consent to a REST API Client tenant-wide. When selected, users don't need to grant client access explicitly to Workday functional areas.
16. From the **Scope (Functional Areas)** prompt, select the functional areas to which your OAuth 2.0 client requires access.

    Select the functional areas that Workday enables for the Workday REST API. Also select the functional areas for the domains of any custom objects to which you might require access. Use caution to expose only those functional areas that you specifically require access to.
17. (Optional) When your OAuth 2.0 client requires access to core Workday domains that aren't in any functional areas, select the **Include Workday Owned Scope** check box.

18. (Optional) When you want Workday to authorize OAuth 2.0 client access only from specified IP address ranges, select the ranges from the **Restricted to IP Ranges** prompt.

    You can also select **Create IP Range** to create a named, comma-separated list of IP addresses using one of these formats:

    - X.X.X.X.
    - CIDR notation. Example: 192.168.0.1/24.
    - X.X.X.X - Y.Y.Y.Y.

    Note: Workday has a limitation on IP ranges that include a dash. If you experience sign-in errors in the **Signons and Attempted Signons** report after you begin using an IP range that you entered in that format:

    a. To see if the range breaks down to a series of smaller segments, use a tool that converts IP address ranges to CIDR notation. Such third-party CIDR calculator tools are available online.
    b. Reenter the **IP Range** in Workday as a comma-separated list of the segments returned by the tool. Example: 199.67.128.0/18, 199.67.192.0/24 or 199.67.128.0-199.67.191.255, 199.67.192.0-199.67.192.255.

19. Add a row to the **Allowed Origin** grid for each domain enabled for cross-origin requests. The domains must start with `https://` or `chrome-extension://` and use the CORS format.

    Workday might add CORS headers when responding to cross-origin requests from **Allowed Origin** domains. Workday only supports cross-origin requests for clients using the Authorization Code grant type with PKCE support.

Result

Workday generates a Client ID and a Client Secret for the OAuth 2.0 client. Copy the Client Secret before you navigate away from the page, and store it securely. If you lose the Client Secret, you can generate a new one using the **Generate New API Client Secret** task.

Workday can deliver OAuth 2.0 clients as part of an update. All OAuth 2.0 clients delivered by Workday are disabled by default.

Next Steps

If you want to generate a new Client Secret for an OAuth 2.0 client:

1. Access the **Generate New API Client Secret** task.
2. Select the **API Client** from the prompt.
3. Select the **Confirm** check box.

Note: When the OAuth 2.0 client is already in use, generating a new Client Secret will cause the client to become unusable.

Related Information
Tasks
Manage API Client Access to Workday on page 81

Register API Clients for Integrations

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

Register API clients for integrations so that you can build integrations on the Workday REST API.

Steps

1. Access the **Register API Client for Integrations** task.
2. Enter the **Client Name**.
3. Select the **Refresh Token Timeout (in days)**. You can select a value between 1 and 365 days. The default value is 30 days.

   To prevent the refresh token from timing out, Workday automatically selects the **Non-Expiring Refresh Tokens** check box. You can also select the **Disabled** check box to prevent the client from requesting access to Workday.
4. From the **Scope (Functional Areas)** prompt, select the functional areas to which your OAuth 2.0 client requires access.

   Select the functional areas that Workday enables for the REST API. Also, select the functional areas for domains of any custom objects to which you might require access. Use caution to expose only those functional areas that you specifically require access to.

   Note: When you plan to use API calls to retrieve data from Workday objects with lookup hierarchy calculated fields, you must register your API client with these scopes:

   - Custom

   to make API calls to get lookup hierarchy calculated fields, you must Organizations and Roles scope.
5. (Optional) If your OAuth 2.0 client requires access to core Workday domains that aren't in any functional areas, select the **Include Workday Owned Scope** check box.
6. (Optional) If you want Workday to authorize OAuth 2.0 client access only from specified IP address ranges, select the ranges from the **Restricted to IP Ranges** prompt.

   You can also select **Create IP Range** to create a named, comma-separated list of IP addresses using one of these formats:

   - X.X.X.X.
   - CIDR notation. Example: 192.168.0.1/24.
   - X.X.X.X - Y.Y.Y.Y.

   Note: Workday has a limitation on IP ranges that include a dash. If you experience sign-in errors in the **Signons and Attempted Signons** report after you begin using an IP range that's in that format:

   a. Use a tool that converts IP address ranges to CIDR notation, and see if the range breaks down to a series of smaller segments. Such third-party CIDR calculator tools are available online.
   b. Reenter the **IP Range** in Workday as a comma-separated list of the segments returned by the tool. Example: 199.67.128.0/18, 199.67.192.0/24 or 199.67.128.0-199.67.191.255, 199.67.192.0-199.67.192.255.

Result

Workday generates an API Client for Integrations with an Authorization Code Grant client grant type and a Bearer access token type. Workday also generates a unique Client ID and Client Secret.

Note: Copy the Client Secret before you navigate away from the page and store it securely. If you lose the Client Secret, you can generate a new one using the **Generate New API Client Secret** task.

You can view API Clients for Integrations on a separate tab of the **View API Clients** report.

Next Steps

Manage the refresh tokens for API clients for integrations for specific Workday accounts.

1. As a related action on the API client for integrations, select **API Client** > **Manage Refresh Tokens for Integrations**.
2. Select the **Workday Account** from the prompt. No more than 1 refresh token can exist for a given integrations API client and Workday account pair.

3. Select **Confirm Delete** or **Generate New Refresh Token** to delete the existing refresh token or generate a new one. You can select both options to delete the existing refresh token and replace it with a new one. Integrations that rely on the refresh token will no longer work unless you update them to use the new token. If you don't select the **Generate New Refresh Token** check box:
   - Workday won't generate a new refresh token.
   - You'll need to run the task again to generate a new one.

Manage API Client Access to Workday

Context

Workday enables Security Administrators to manage API client access for users, so that they can view who is actively using OAuth applications and revoke an application's access to Workday if needed. Workday also provides users with a self-service task to manage the API clients in use for their own Workday account and to revoke an application's access to Workday if needed.

Steps

1. To manage API client access to Workday, use the appropriate task:
   - To manage API client access for users, access the **Maintain API Client Access** task. This task is secured to the *Security Administration* security domain.

     This task displays a list of API clients, the scope (functional area) or scopes of each client's access to Workday, and the Workday account that is using each client.
   - To manage API clients in use for your own Workday account, access the **Manage My API Client Applications** task. This task is available by selecting **Workday Account** > **Manage My API Client Applications** as a related action from your Professional Profile, and is secured to the *Core Navigation* security domain.

     This task displays the API clients in use for your Workday account, and the scope (functional area) of each client's access to Workday.
2. Select the **Revoke** check box to revoke an API client's access to Workday. Note that revoking client access to Workday will prevent the user from using that client unless they re-authenticate with Workday.
3. Click **OK**.

Related Information
Tasks
Register API Clients on page 76

Troubleshooting: OAuth 2.0 Authorization Endpoint Errors

This topic provides strategies for diagnosing and resolving errors that occur when your application makes requests to the authorization endpoint of the authorization server:

- Authorization server returns an access_denied error. on page 81
- Authorization server returns an invalid_request error. on page 82
- Authorization server returns an unauthorized_client error. on page 82

The authorization server returns these errors in the **Redirection URI** specified for the API client.

Authorization server returns an access_denied error.

Solution: Perform these actions individually, checking your result each time, until you resolve the issue:

- Check in the **View API Clients** report if Workday locked out the API client due to too many failed sign-in attempts. This condition clears after the lockout period expires for the client. The **View API Clients** report displays the lockout period end time for the client.

- Reissue the authorization request to the authorization server endpoint, and ensure that the resource owner enables access to the specified Workday data. Access the **Maintain API Client Access** task to view the Workday accounts that currently allow access to the API client.
- Access the **Edit API Client** task and clear the **Disabled** check box for the API client if it's selected.
- Access the **Edit Tenant Setup - Security** task and select the **OAuth 2.0 Clients Enabled** check box if it isn't selected.

Authorization server returns an invalid_request error.

Solution: Perform these actions individually, checking your result each time, until you resolve the issue:

- Ensure that the grant_type in the access token request is correct and is 1 of the grant types supported by Workday.
- If the grant_type in the access token request is authorization_code, ensure that the code isn't empty or greater than 32 characters.

Authorization server returns an unauthorized_client error.

Solution: Ensure that the response_type in the authorization request is correct for the API client grant type. Example: Ensure that response_type=code if the API client **Client Grant Type** is **Authorization Code Grant**.

Troubleshooting: OAuth 2.0 Token Endpoint Errors

This topic provides strategies for diagnosing and resolving errors that occur when your application makes requests to the token endpoint of the authorization server:

- Authorization server returns an invalid_client error. on page 82
- Authorization server returns an invalid_grant error. on page 83
- Authorization server returns an invalid_request error. on page 84

Authorization server returns an invalid_client error.

Solution:

Steps

1. Access the **Signons and Attempted Signons** report, and select the **Show Signon Attempts with an Invalid User Name** check box.

   Security: These domains in the System functional area:

   - *Workday Account Monitoring*
   - *Workday Accounts*
2. Search the **Signon Attempts with an Invalid User Name** tab for records where:
   - **Attempted Authentication Type** is OAuth 2.0.
   - **Authentication Failure Message** is populated.
3. Match the failure message displayed in the report with the solution in this table.

Failure Message	Solution
Authorization header was not provided or was incorrect on access token request.	Ensure that the authorization header: • Is included in the access token request. • Is in the form client_id:client_secret in Base64 encoded format.
Client for access token request is currently locked out.	Workday locked out the API client due to too many failed sign-in attempts. This condition clears after

Failure Message	Solution
	the lockout period expires for the client. Access the **View API Clients** report to view the lockout period end time for the client.
Client for access token request is disabled.	**1.** Access the **Edit API Client** task. Security: *Security Administration* domain in the System functional area. **2.** Select the API client making the access token request. **3.** Clear the **Disabled** check box, if selected.
No client was found for the client ID provided in the access token request.	Ensure that the client_id in the access token request is correct.
OAuth 2.0 is disabled for this tenant; access token request rejected.	**1.** Access the **Edit Tenant Setup - Security** task. Security: *Set Up: Tenant Setup - Security* domain in the System functional area. **2.** Select the **OAuth 2.0 Clients Enabled** check box, if cleared.
Provided client secret was incorrect for access token request.	Ensure that the client_secret in the access token request is correct.

Authorization server returns an invalid_grant error.

Solution:

Steps

1. Access the **Signons and Attempted Signons** report, and select the **Show Signon Attempts with an Invalid User Name** check box.

   Security: These domains in the System functional area:

   - *Workday Account Monitoring*
   - *Workday Accounts*
2. Search the **Signon Attempts with an Invalid User Name** tab for records where:
   - **Attempted Authentication Type** is OAuth 2.0.
   - **Authentication Failure Message** is populated.
3. Match the failure message displayed in the report with the solution in this table.

Failure Message	Solution
Provided grant for access token request was expired or invalid.	Obtain a new authorization code to use in the access token request. Authorization codes expire after 10 minutes.
Provided grant for access token request was not found.	Ensure that the authorization code in the access token request is: • Correct. • Hasn't expired. • Hasn't already been used.

Failure Message	Solution
Provided grant for access token request was not issued to the client corresponding to the given client credentials.	Ensure that the client_id and client_secret in the access token request belongs to the client to which the authorization server issued the authorization code.
System Account disabled.	1. Access the **Edit Workday Account** task. 2. Enable the resource owner's account, if it's unnecessarily disabled. See Edit Workday Accounts on page 246.
System Account expired.	1. Access the **Edit Workday Account** task. 2. Reset the resource owner's **Account Expiration Date**, if it's unnecessarily expired. See Edit Workday Accounts on page 246.
System Account locked.	1. Access the **Manage Workday Accounts** task. 2. Unlock the resource owner's account, if it's unnecessarily locked. See Lock and Unlock Workday Accounts on page 258.
System Account locked out.	The resource owner's account is locked due to too many failed sign-in attempts. This condition clears after the lockout period expires for the account. Access the **Workday Accounts Currently Locked Out By Excessive Failed Signon Attempts** report to view the lockout period end time for the account.
System Account not found.	You must use an ISU account with the JWT Grant Type.

Authorization server returns an invalid_request error.

Solution: Perform these actions individually, checking your result each time, until you resolve the issue:

- Ensure that you include the grant_type parameter in the access token request.
- Ensure that you include the authorization code (code) parameter in the access token request.

Related Information
Reference
Troubleshooting: OAuth 2.0 Authorization Endpoint Errors on page 81

Authentication Examples

Example: Administrator Access on Corporate Network Only

This example illustrates 1 way to configure an authentication policy that enables administrator and manager access from the corporate network only.

Context

You want to enable all users to perform self-service tasks from any network or location using SAML authentication. However, you want HR administrators and managers to access Workday from your corporate network only when they perform tasks that require additional permissions, such as:

- Pay rate changes.
- Team calibration.

Prerequisites

You must have security administrator privileges.

Steps

1. Create role-based security groups (unconstrained) for administrators and managers, such as:
   - *HR Administrators*
   - *HR Partner*
   - *Manager*
2. Access the **Manage Authentication Policies** report.
3. Create a new authentication policy or edit an existing one.
4. Click **Manage Networks** to access the **Maintain IP Ranges** task, and define your corporate network by listing 1 or more ranges of IP addresses for your network.

Option	Description
Display Name	Corporate HQ
IP Range	192.0.2.0/24

5. Add rows in the **Authentication Ruleset** grid and define these rules:

Option	Description
Authentication Rule Name	*HR and Managers Rule*
Security Group	• *HR Administrator* • *HR Partner* • *Manager*
Authentication Condition	*Corporate HQ*
Allowed Authentication Types	*SAML*
Access Restriction for Authentication Condition	*Supported Workers* (See the next step to create.)

Option	Description
Authentication Rule Name	*Worker Self-Service Rule*
Security Group	• *All Employees* • *All Contingent Workers*
Authentication Condition	*Any*
Allowed Authentication Types	*SAML*
Access Restriction for Authentication Condition	*Self-Service* (See the next step to create.)

6. To define an access restriction, from the **Access Restriction for Authentication Condition** prompt for the appropriate rule, click **Create**.

   For the *HR and Managers Rule*:

Option	Description
Name	*Supported Workers*
Allows Access to Security Groups	*Any Organization Role (Leadership or Supporting)*

   For the *Worker Self-Service Rule*

Option	Description
Name	*Self-Service*
Allows Access to Security Groups	• *All Employees* • *Contingent Worker As Self* • *Employee As Self*

7. In the **Default Rule for All Users** grid, select the **Disabled** check box.
8. Access the **Domain Security Policies for Functional Area** report for the Staffing functional area.
9. Configure the *Worker Data: Public Worker Reports* domain security policy to grant **View** access to the All Employees security group.
10. Access the **Activate Pending Security Policy Changes** task to confirm the security policy changes.
11. Access the **Activate All Pending Authentication Policy Changes** task to confirm the authentication policy changes.

Result

All workers can perform self-service tasks from any network. HR administrators, HR partners, and managers can perform tasks related to their assigned groups, only if they sign in to the corporate network.

Related Information

Tasks

Add Authentication Rules on page 8
Create Access Restrictions on page 12
Maintain IP Ranges on page 11

Example: All Access from Corporate Network Only

This example illustrates 1 way to configure an authentication policy that restricts all Workday access to the corporate network only.

Context

You want users to access Workday from within your corporate network only using Workday user name password authentication. You enable most users to access Workday with username and password only. However, you require multifactor authentication for these users with job descriptions that grant them additional permissions to support their assigned teams:

- HR administrators.
- HR partners.
- Managers.

Prerequisites

- Select and approve a third-party authenticator app.

- Security: *Security Configuration* and *Set Up: Tenant Setup - Security* domains in the System functional area.

Steps

1. Create role-based security groups (unconstrained) for administrators and managers, such as:
   - HR Administrator.
   - HR Partner.
   - Manager.
2. Access the **Edit Tenant Setup - Security** task.
3. On the **Multi-Factor Authentication Providers** grid, click **Add Multi-Factor Authentication Provider** and add these authentication providers to the tenant:
   - **Authenticator App**.
   - (Optional) **Backup Codes**.
4. Click **OK** and **Done**.
5. Access the **Manage Authentication Policies** report.
6. Create a new authentication policy or edit an existing one.
7. Click **Manage Networks**. In **Maintain IP Ranges**, define your corporate network by listing 1 or more ranges of IP addresses for your network.

Option	Description
Display Name	Corporate HQ
IP Range	192.0.2.0/24

8. Click **OK**.
9. Add a row in the **Authentication Ruleset** table and add this rule:

Option	Description
Authentication Rule Name	HR and Managers Rule
Security Group	*HR Administrator* *HR Partner* *Manager*
Authentication Condition	*Corporate HQ*
Allowed Authentication Types	*User Name Password*
Multi-factor Authentication	*Authenticator App* *Backup Codes*

10. In the **Default Rule for All Users** table, add a condition for the *Default Rule*:

Option	Description
Authentication Rule Name	Default Rule
Security Group	*All Users*
Authentication Condition	*Corporate HQ*
Allowed Authentication Types	*User Name Password*

11. Click **OK** and **Done**.
12. Access the **Activate All Pending Authentication Policy Changes** task to activate and confirm the changes.

Result

All users can access Workday, only if they are on the corporate network. Most workers can access Workday by signing in with their Workday username and password only. Workday also requires HR administrators, HR partners, and managers to authenticate using an authenticator app.

Related Information
Tasks
Add Authentication Rules on page 8
Create Role-Based Security Groups on page 174
Maintain IP Ranges on page 11

Example: All Access from Managed Devices Only

This example illustrates 1 way to configure an authentication policy that restricts all Workday access to be from managed devices only. A managed device in this context is a device that a third-party mobile device management (MDM) provider administers for your organization.

Context

You want all of your users to access Workday in your Production environment using SAML from managed devices. Users must access Workday from within your corporate network to perform most tasks, but can access Workday from any network to perform self-service tasks.

Prerequisites

You must:

- Have security administrator privileges.
- Obtain the name of the Managed Device Attribute from your SAML provider.
- Provide a list of managed devices to your SAML provider, and keep it current.

Steps

1. Access the **Edit Tenant Setup - Security** task.
2. Select the **Enable SAML Authentication** check box.
3. In the **SAML Identity Providers** grid, add a row for the identity provider (IdP) you want to use for SAML authentication.

   Enter the managed device attribute that you obtained from your SAML provider into the **Managed Device Attribute** field for the IdP.
4. Click **OK** and **Done**.
5. Access the **Manage Authentication Policies** report.
6. Disable any authentication policy currently enabled for the Production environment.
7. Click **Add Authentication Policy** and enable the new authentication policy for the Production environment.

Option	Description
Restricted to Environment	*Production*
Authentication Policy Enabled	Selected.

8. Click **OK** and **Done**.
9. Click **Edit**, and then **Manage Networks**.

10. In **Maintain IP Ranges**, define your corporate network by listing 1 or more ranges of IP addresses for your network.

Option	Description
Display Name	Corporate HQ
IP Range	192.0.2.0/24

11. Click **OK** and **Done**.
12. Click **Edit**, add a row in the **Authentication Ruleset** table, and add this rule:

Option	Description
Authentication Rule Name	Default Rule for All Users
Security Group	*All Users*
Authentication Condition Name	Condition-a
Allowed Authentication Types	*SAML*
Authentication Condition	*Corporate HQ* **Device is Managed** selected.

13. Add a second condition to the same rule:

Option	Description
Authentication Condition Name	Condition-b
Allowed Authentication Types	*SAML*
Authentication Condition	*Any* **Device is Managed** selected.
Access Restriction for Authentication Condition	*Self-Service* (See next step to create.)

14. To define an access restriction, from the **Access Restriction for Authentication Condition** prompt for the second condition of the *Default Rule for All Users*, click **Create Access Restriction**.

Option	Description
Name	Self-Service
Allows Access to Security Groups	• *Employee As Self* • *Contingent Worker As Self*

15. In the **Default Rule for All Users** grid, select the **Disabled** check box.
16. Click **OK** and **Done**.
17. Access the **Activate All Pending Authentication Policy Changes** task to activate and confirm the changes.

Result

Users can access Workday only if they're doing so from a managed device using SAML authentication. Users can access self-service tasks from any network. They must, however, access Workday from the corporate network to perform other tasks.

Example: Emergency Sign-In for Administrators

This example illustrates 1 way to configure an authentication policy that enables a user-based security group to access Workday directly in case the SSO provider goes offline.

Context

Your organization uses a SAML Single Sign-On provider, and you require all workers to sign in through this provider. However, you want to ensure that at least 2 administrators in your organization have access to Workday if the servers of the SSO provider go offline unexpectedly. These 2 administrators can perform critical tasks, such as:

- Payroll processing on payday.
- Temporarily modifying the authentication policy so that HR administrators and C-level executives can sign in to Workday to perform critical tasks.

Prerequisites

- You must have security administrator privileges.
- Select and approve a third-party authenticator app.

Steps

1. Create a role-based or user-based security group *Emergency Administrators* for 2 or more administrators who would be the first responders in case your SSO provider goes offline.
2. Access the **Edit Tenant Setup - Security** task.
3. On the **Multi-Factor Authentication Providers** grid, click **Add Multi-Factor Authentication Provider** and add these authentication providers to the tenant:
   - **Authenticator App**
   - (Optional) **Backup Codes**
4. Click **OK** and **Done**.
5. Access the **Manage Authentication Policies** report.
6. Create a new authentication policy or edit an existing one.
7. Click **Manage Networks**. In **Maintain IP Ranges**, define your corporate network by listing 1 or more ranges of IP addresses for your network.

Option	**Description**
Display Name	Corporate HQ
IP Range	192.0.2.0/24

8. Click **OK**.
9. Add rows in the **Authentication Ruleset** grid and add these rules:

Option	**Description**
Disabled	(unchecked)
Authentication Rule Name	Emergency Level 1 Rule
Security Group	*Emergency Administrators*
Authentication Condition	*Corporate HQ*
Allowed Authentication Types	*SAML* *User Name Password*
Multi-factor Authentication	*Authenticator App*

Option	Description
	Backup Codes

Option	Description
Disabled	(checked)
Authentication Rule Name	Emergency Level 2 Rule
Security Group	*HR Administrator* *Chief Executive Officer* *Chief Financial Officer*
Authentication Condition	*Corporate HQ*
Allowed Authentication Types	*SAML* *User Name Password*
Multi-factor Authentication	*Authenticator App* *Backup Codes*

Option	Description
Disabled	(unchecked)
Authentication Rule Name	Default Rule for All Workers
Security Group	*All Employees* *All Contingent Workers*
Authentication Condition	*Any*
Allowed Authentication Types	*SAML*

Emergency Level 2 Rule is an optional rule that you can set up ahead of time to enable the same sign-in options for:

- HR administrators.
- C-level managers.

Disable this rule. The *Emergency Administrators* can temporarily enable it during the emergency.

Default Rule for All Workers must be the last rule in the list.

For greater security with the *Emergency Level 1 Rule* and *Emergency Level 2 Rule*:

- Set the allowed networks (under **Authentication Condition**) to the corporate network.
- Select multifactor authentication (**Authenticator App**, and optionally **Backup Codes**).

10. In the **Default Rule for All Users**, select the **Disabled** check box.
11. Click **OK** and **Done**.
12. Access the **Activate All Pending Authentication Policy Changes** task to activate and confirm the changes.
13. Verify that the *Emergency Administrators* group has sufficient permissions to modify authentication policies to enable other workers to access Workday temporarily.

Result

If the SSO provider goes offline, the members of *Emergency Administrators* can sign in to Workday to perform tasks or to modify authentication policies.

Related Information
Tasks
Add Authentication Rules on page 8
Maintain IP Ranges on page 11

Example: Non-SSO Access for Pre-Hires

This example illustrates 1 way to configure an authentication policy that enables pre-hires to access Workday without signing in through your Single Sign-On (SSO) provider.

Context

Your organization uses a SAML SSO solution to access multiple services, including Workday. You need to enable pre-hires to perform self-service tasks, such as updating their personal information or performing onboarding tasks before their start date. However, you don't want them to sign in through your SAML SSO, which might give them premature access to all worker services.

Prerequisites

You must have security administrator privileges.

Steps

1. Access the **Manage Authentication Policies** report.
2. Create a new authentication policy or edit an existing one.
3. Add a row in the **Authentication Ruleset** table and add these rules:

Option	Description
Security Group	*All Pre-Employees* *All Pre-Contingent Workers*
Authentication Condition	*Any*
Allowed Authentication Types	*User Name Password*

Option	Description
Security Group	*All Employees* *All Contingent Workers*
Authentication Condition	*Any*
Allowed Authentication Types	*SAML*

4. In the **Default Rule for All Users**, select the **Disabled** check box.
5. Click **OK** and **Done.**
6. Access the **Activate All Pending Authentication Policy Changes** task to activate and confirm the changes.

Result

Workday requires all workers to sign in using their SAML SSO account, whereas Workday requires pre-hires to sign in with their Workday username and password.

Related Information
Concepts
Concept: Security Groups on page 129
Tasks
Add Authentication Rules on page 8
Steps: Set Up SAML Authentication on page 46

Example: Passwordless Sign-In for Employees and Contingent Workers

This example illustrates how to configure an authentication policy that enables employees and contingent workers to:

- Enroll WebAuthn credentials.
- Sign in using Workday passwordless sign-in.

Context

You want to enable all employees and contingent workers in your organization to use passwordless sign-in as a method of accessing their Workday accounts. You want all other accounts to use user name password authentication to access Workday.

Note: Workday doesn't support passwordless sign-in, also known as web authentication, as a primary authentication type on the Workday mobile apps.

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Steps

1. Manage passwords for the tenant.

   Set up password rules and reset options. Your users must maintain an account password since they need to be able to sign in to Workday with their password to set up passwordless sign-in.
2. Access the **Edit Tenant Setup - Security** task, and select the **Enable Web Authentication** check box.
3. Click **OK** and **Done**.
4. Access the **Manage Authentication Policies** report.
5. Create a new authentication policy or edit an existing one.
6. Add a row in the **Authentication Ruleset** table and add this rule:

Option	Description
Authentication Rule Name	Employees and Contingent Workers Rule
Security Group	*All Employees* *All Contingent Workers*
Allowed Authentication Types	*User Name Password* *WebAuthn (FIDO2)*

7. In the **Default Rule for All Users** table, add a condition for the *Default Rule*:

Option	Description
Authentication Rule Name	Default Rule
Security Group	*All Users*
Allowed Authentication Types	*User Name Password*

8. Click **OK** and **Done**.
9. Access the **Activate All Pending Authentication Policy Changes** task to activate and confirm the changes.

Result

Workday prompts employees and contingent workers to set up passwordless sign-in after they sign in with their username and password. If they set it up, Workday prompts them to register their authenticator for their account.

Once they've registered their authenticator, the next time they sign in, they can:

- Click the **Passwordless Sign In** link and sign in using their registered authenticator.
- Sign in with their username and password.

Next Steps

Users can access the **Manage Passwordless - Webauthn (FIDO2) Credentials** report to view a list of their registered credentials, and remove credentials they want to unregister. They can use the **Manage Security Settings** report to access the **Manage Passwordless - Webauthn (FIDO2) Credentials** report.

Related Information
Tasks
Add Authentication Rules on page 8
Steps: Manage Passwords on page 243
Reference
Reference: Edit Tenant Setup - Security

Example: Virtual Clean Room (VCR) Restricted Implementer Access for IP-Restricted Tenants

This example illustrates how to ensure that VCR-restricted Workday implementers have access to a tenant when the authentication policy restricts Workday access to a specific network.

Note: This example uses user name password as the authentication type. You can configure other authentication types, some of which require additional configuration.

Context

You want your company employees to access Workday only from within your corporate network. You also need to ensure that:

- VCR-restricted implementers can also access Workday, since such users can only get access through Workday-assigned IP addresses that aren't in your corporate network.
- Other implementers that aren't VCR-restricted can access Workday only through a network address that you assign, which isn't in your corporate network.

Steps

1. Access the **Manage Authentication Policies** report.
2. Create a new authentication policy or edit an existing one.
3. Click **Manage Networks**. In **Maintain IP Ranges**, define your corporate network.

Option	Description
Display Name	Corporate Network
IP Range	192.0.2.0/24

4. Define a separate network that non VCR-restricted implementers will use.

Option	Description
Display Name	Implementer Network
IP Range	192.0.3.12

5. Click **OK**.
6. Add rows in the **Authentication Ruleset** table to define these rules:

Option	Description
Authentication Rule Name	VCR-Restricted Implementers
Security Group	*All VCR Restricted Implementers*
Authentication Condition	*Any*
Allowed Authentication Types	*User Name Password*

Option	Description
Authentication Rule Name	Other Implementers
Security Group	*All Non-VCR Restricted Implementers* *Implementers*
Authentication Condition	*Implementer Network*
Allowed Authentication Types	*User Name Password*

Option	Description
Authentication Rule Name	Employees
Security Group	*All Employees*
Authentication Condition	*Corporate Network*
Allowed Authentication Types	*User Name Password*

7. **Order** the rules in the **Authentication Ruleset** grid in this hierarchy:
   a. **VCR-Restricted Implementers**.
   b. **Other Implementers**.
   c. **Employees**.
8. Click **OK** and **Done**.
9. Access the **Activate All Pending Authentication Policy Changes** task to activate and confirm the changes.

Related Information
Concepts
Concept: Authentication Policy Best Practices on page 16

Monitoring Sign Ins

Enable Users to View Their Sign-In History

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can enable users to access the **View Signon History** report so that they can:

- Review their own Workday sign-in activity for a selected time period.
- Identify any suspicious sign-in activity for their Workday account.

Steps

1. Access the **Domain Security Policies for Functional Area** report for the System functional area.
2. Configure the *Self-Service: Signons* domain security policy.
   Grant **View** access to 1 or both of these security groups:
   - Employee as Self
   - Contingent Worker as Self
3. Access the **Activate Pending Security Policy Changes** task to confirm changes.

Result

Users can access the **View Signon History** report and review details about their sign-in activity such as:

- Sign in and sign out times.
- Device type.
- Authentication type.
- IP address.

They can use the **Manage Security Settings** report to access the **View Signon History** report.

Authentication types in the **View Signon History** report include:

- Proxy.
- User name and password.
- Workday Central Login.

Next Steps

If users identify suspicious sign-in activity, they can access the **Manage Active UI Sessions** report and click **End All Active UI Sessions**. This action immediately ends all UI sessions other than their current session.

Related Information
Tasks
Edit Domain Security Policies on page 200

Reference: Signons and Attempted Signons Report

The **Signons and Attempted Signons** report (secured to the *Workday Account Monitoring* and *Workday Accounts* domains) provides a history of user sign-ins during a specified time period.

You can use a security analysis tool with this report to more easily detect possible threat patterns in the data. Consult a network security expert to perform a comprehensive analysis of this report. You can also use this report when changing authentication settings to verify that the settings are working properly.

Note: Workday returns up to 50,000 rows in the **Signons and Attempted Signons** report, beginning with the oldest sign-in records within the time period you specify. If the sign-in history contains more than 50,000 records, you might be missing some records. If the report returns 50,000 rows, Workday recommends that you adjust the **From Moment** and **To Moment** values to ensure you capture the sign-in records you need. The 50,000 row limit applies whether the report displays in the UI or runs as a background process.

If you select the **Show Signon Attempts with an Invalid User Name** check box, Workday includes an additional tab for the report, with details about unidentified sign-in attempts.

When reviewing the report, consider:

Field	Description
Signon	Links to the **View System Account Signon** report, which includes: • The raw request payload for SAML and OpenID sign-in attempts whether successful or not. • The relevant authentication policy components, such as **Matching Authentication Rule** and **Matching Authentication Type Restriction**.
Session Start **Session End**	Times are based on the Workday server time.
Workday Account	If the Authentication Type is **Proxy**, this field also includes: • The Workday Support account. • The account used as a proxy for troubleshooting user account issues.
Invalid Credentials	Indicates if authentication failed due to an invalid: • Password. • One-time passcode. • Answer to a challenge question. • SAML token. • X.509 certificate. A blank value doesn't necessarily indicate that the credentials are valid.
Forgotten Password Reset Request	The **Authentication Failure Message** field provides details about the failure. Example: A user clicks the **Forgot Password** link but incorrectly answers their challenge questions.
Required Password Change	The administrator requires the user to change their password at next sign-in.
Authentication Failure Message	Indicates why the sign-in attempts failed, such as if it failed due to privileged access or network

Field	Description
	limitations. Example: Virtual clean room (VCR) restrictions set for your tenant.
Authentication Channel	Indicates the authentication channels used at sign-in.
ID	This field is empty if Workday didn't successfully authenticate the user.

Authentication Types for Signon
This table lists the authentication types that are possible for the specified authentication channel.

Authentication Channel	Authentication Type for Signon
Internal	• OAuth 2.0.
UI	• Biometric. • Mobile PIN. • OAuth 2.0. • OpenID Connect. • Proxy. (Workday Support signed in through the account of a user, on behalf of that user, for troubleshooting. For Workday internal use only.) • SAML. • User Name Password + Challenge Questions. • WebAuthn (FIDO2).
UI, Web Services	• User Name Password. (Standard authentication type. Includes Delegated Authentication.)
Web Services	• Trusted (Workday signed a Workday system account to perform internal tasks. For Workday internal use only.) • X.509

Related Information
Concepts
Concept: SAML Authentication on page 61
Concept: X.509 Certificates in Workday on page 230
Tasks
Steps: Set Up Mobile Authentication
Enable OpenID Connect Authentication on page 73
Manage Challenge Questions on page 32
Register API Clients on page 76
Steps: Set Up Delegated Authentication on page 69

Reference: Account Access Reports

Workday provides various reports for tracking user account access.

You can search for and access these reports in Workday.

Report	Security
Active Sessions	Secured to the *Workday Accounts* domain in the System functional area.
Manage Active UI Sessions	Secured to these domains in the System functional area: • *Self-Service: Account* • *Self-Service: Security Actions*
Workday Accounts	Secured to the *Workday Accounts* domain in the System functional area.
Signons and Attempted Signons	Secured to these domains in the System functional area: • *Workday Account Monitoring* • *Workday Accounts*
Workday Accounts Currently Locked Out by Excessive Failed Signon Attempts	Secured to the *Workday Accounts* domain in the System functional area.
Workday Accounts Currently Locked Out by Effective Moment Signon Attempts	Secured to the *Workday Accounts* domain in the System functional area.
Workday Accounts With Expired Passwords	Secured to the *Workday Accounts* domain in the System functional area.

You can access these reports from a worker's related actions menu:

Report	Security and Access
Signon History for Person	Secured to the *System Auditing* domain in the System functional area. Select **Security Profile > View Signon History**.
Update Audit for User	Secured to the *System Auditing* domain in the System functional area. Select **Security Profile > View Update Audit**.
Workday Account for Person	Secured to these domains in the System functional area: • *Security Administration* • *Workday Accounts* Select **Security Profile > View Workday Account**.

Proxy Access to Non-Production Tenants

Manage Proxy Access

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can provide proxy access to your non-Production Workday environment for certain users. Proxy access policies specify:

- The non-Production environments to which the proxy access policy applies.
- The security groups whose members have proxy access to Workday.
- The security groups containing members on whose behalf users can act when they're signed in to Workday.
- (Optional) The security groups containing members who can't have proxy access to Workday.

A user can't perform delegated tasks when signed in to Workday as a proxy user. If a user is subject to access restrictions, those restrictions remain in effect when that user acts on behalf of another user.

Steps

1. Access the **Create Proxy Access Policy** task.
2. As you complete the task, consider:

Option	Description
Restricted to Environment	The environments to which the proxy access policy applies. You can only have 1 proxy access policy for any Workday environment. You can't select your Production environment. **Note:** To apply the proxy access policy to your Sandbox Preview or Implementation Preview tenant, select *Sandbox* or *Implementation* respectively at the **Restricted to Environment** prompt. Those environments also apply to the respective preview tenants.
Do Not Allow Proxy on Behalf Of	(Optional) The security groups containing members on whose behalf another user can't sign in to Workday as a proxy user.
Groups That Can Proxy	The security groups containing members for whom you want to enable proxy access according to that rule. You can only enable proxy access to unconstrained security groups. Example: To grant proxy access to all HR Partners, create a Role-Based security group (Unconstrained) for the HR Partner role and select that security group from the prompt.
On Behalf Of	The security groups containing members on whose behalf users belonging to the **Groups That Can Proxy** will be able to act.

Result

Members of security groups listed in the **Groups That Can Proxy** field can now act as proxies on behalf of members of security groups listed in the **On Behalf Of** field for the rules in the policy.

Note: If a user isn't able to proxy on behalf of another user, and:

- The environment is correct.
- The **On Behalf Of** user isn't in a security group listed in the **Do Not Allow Proxy on Behalf Of** field.

Ensure that the account of the **On Behalf Of** user isn't locked, disabled, or expired, and that the account password isn't expired. Run the **All Workday Accounts** report to check the status of the account.

Next Steps

View details about users starting and stopping proxy sessions on the **Signons and Attempted Signons** report.

Related Information

Examples

Example: Create a Proxy Access Policy on page 102

Concept: Proxy Sessions

You can start and stop proxy sessions in your nonproduction Workday environment if:

- Workday has a proxy access policy in place.
- You have proxy access to Workday according to one of the rules in the proxy access policy.

You start and stop proxy sessions by accessing the **Start Proxy** and **Stop Proxy** tasks.

During a proxy session:

- Workday displays **On Behalf of** and the name of the user on whose behalf you're acting.
- You can perform actions in Workday that Workday authorizes the user you're proxying for to perform. Proxy sessions do exclude certain functionality, however.

Importance of Rule Order in Proxy Sessions

In a proxy access policy, order rules:

1. From the most restrictive rule, at the top of the rule list.
2. To the least restrictive rule, at the bottom of the rule list.

You need to set up rules this way because of the way Workday tests and evaluates rules:

1. When a user starts a proxy session, Workday tests the rules starting at the top of the list.
2. Once Workday finds a relevant rule, it evaluates the rule. If any security groups of the current user match any **Groups That Can Proxy**, Workday enables proxy access. If Workday doesn't find a match, it denies proxy access.

   A rule is relevant if the user on whose behalf the current user wants access is a member of a security group listed in **On Behalf Of**.
3. Once Workday evaluates a rule, it doesn't test the other rules below it in the rule list.

Note: A rule that is relevant to a large number of Workday users is less restrictive than one that is relevant to a relatively small number of users. Example: A rule enables proxy access on behalf of Workday users in the All Employees security group. That rule is less restrictive than a rule that enables proxy access on behalf of Workday users in the Accountant (Unconstrained) security group.

Excluded Functionality

A proxy session excludes access to certain Workday functionality as well as functionality that requires connecting to another service, including:

- Access to documents on **My Reports**.
- Background conversions.
- Business form printing.
- Delegated business process tasks.
- Email.
- Integrations (including Reports as a Service, REST API, and Workday Studio).

- Knowledge Management.
- Mass Actions
- Mobile Push Notifications.
- Notifications received through the user interface.
- Org Studio
- **Quick Tasks** on the People Experience Home page.
- Scheduled reports.
- Securable items configured on the **Favorites** worklet.
- Solutions.
- Updates to **Evaluated By** field in employee reviews.
- Workday Assistant.

You can print reports or run integrations if the account you're acting on behalf of has permissions to run the report or integration. In such cases, the account you're proxying for runs the print or integration as if there's no proxy session. Example: Logan McNeil signs in, starts a proxy session acting as Betty Liu, and prints a report. While proxied, the print runs using Betty Liu's account as if there's no proxy session. The print succeeds if Betty Liu has permissions to run the report.

Passwordless Sign-In

Workday doesn't support passwordless sign-in, also known as web authentication, for proxy sessions.

Monitor Proxy Access

View the actions taken during a proxy session in the audit trail for the user on whose behalf you're acting. You can view details about users starting and stopping a proxy session on the **Signons and Attempted Signons** report.

Example: Create a Proxy Access Policy

This example illustrates how to create a proxy access policy in Workday. The policy enables certain Workday users to access and perform tasks on behalf of other Workday users.

Context

You want to create a proxy access policy that enables:

- Susan Thomasson, the Operations Executive, to access Workday on behalf of Steve Morgan, the CEO.
- Logan McNeil, the HR Administrator, to access Workday on behalf of Dawn Myers, an HR partner.
- Dawn Myers to access Workday on behalf of Olivia Price, a contingent worker.

For this scenario, all of these Workday users must be in the security groups that are relevant to their job titles. All of them except Olivia Price must also be in the *All Employees* security group.

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Create an unconstrained role-based security group named HR Partner that includes the HR Partner role.

Steps

1. Access the **Create Proxy Access Policy** task.
2. Select your environment in the **Restricted to Environment** field.

3. Create these rules in the rules grid in the order shown:

Groups That Can Proxy	On Behalf Of
Operations Executive	Chief Executive Officer
HR Administrator	HR Partner
HR Partner	All Contingent Workers All Employees

Result

Workday enables proxy access for all 3 users because the rules are in order from the most restrictive rule at the top of the list to the least restrictive rule at the bottom of the list.

Related Information
Tasks
Manage Proxy Access on page 99

Authentication References

Reference: Workday Sign In URLs

Workday URLs use this format on any device:

`https://<workdayhost>/<tenantname>/<path>`

Specific URLs for accessing Workday vary depending on:

- Your authentication configuration.
- How users access Workday.

Workday Host

The `<workdayhost>` indicates:

- The tenant environment you're accessing.
- The location of the Workday Data Center for your tenant.

For Production environments:

Data Center	Workday Host
WD1	`www.myworkday.com`
WD3	`wd3.myworkday.com`
WD5	`wd5.myworkday.com`
WD10	`wd10.myworkday.com`
WD12	`wd12.myworkday.com`
WD102	`wd102.myworkday.com`
WD103	`wd103.myworkday.com`
WD104	`wd104.myworkdaygov.com`
WD105	`wd105.myworkday.com`

For non-Production environments (Sandbox, Sandbox Preview, Implementation, and Implementation Preview):

Data Center	Workday Host
WD2	`impl.workday.com`
WD3	`wd3-impl.workday.com`
WD5	`wd5-impl.workday.com`
WD10	`impl.wd10.myworkday.com`
WD12	`impl.wd12.myworkday.com`
WD102	`impl.wd102.myworkday.com`
WD103	`impl.wd103.myworkday.com`
WD104	`impl.wd104.myworkdaygov.com`
WD105	`impl.wd105.myworkday.com`

Tenant Name

The tenant name is a unique identifier that someone assigns to the tenant of your organization during implementation. You can also select additional tenant names (aliases).

Because non-Production environments use the same `<workdayhost>` according to the data center, use `<tenantname>` to differentiate between these environments.

Environment	Format
Sandbox	`<tenantname>`
Sandbox Preview	`<tenantname>_preview`
Implementation, Implementation Preview	`<tenantname>`x, where x is the tenant number.

Replace `<tenantname>` with the original tenant name or an alias that is appropriate for the tenant you're accessing.

Example: If your tenant name is `abc`, your Sandbox Preview tenant would be `abc_preview`, and your first 3 Implementation tenants would be `abc1`, `abc2`, and `abc3`.

Path

If you're using Workday authentication, users directly sign in to Workday. If you're using Single Sign-On (SSO), you need to provide the Workday endpoint URLs to your identity provider (IdP) to redirect users after they authenticate.

Authentication Type	Path
Workday authentication	`login.htmld`
SAML	`login-saml.htmld`
OpenID Connect	`login-oidc-auth.htmld`

- If your second Implementation Preview tenant (`acme2`) is in Dublin (`wd3-impl.workday.com`) and you use Workday authentication (`login.htmld`), use this URL to access Workday: `https://wd3-impl.workday.com/acme2/login.htmld`.
- If your Production tenant (`abc`) is in Portland (`wd5.myworkday.com`) and you use SAML authentication (`login-saml`), use this URL to access Workday: `https://wd5.myworkday.com/abc/login-saml.htmld`.

Related Information

Concepts

Concept: SAML Authentication on page 61

Tasks

Steps: Set Up Workday Mobile Applications

Reference

Workday Data Centers

Reference: Edit Tenant Setup - Security

FAQ: Authentication

Where can I see who attempted to sign in to Workday and whether their attempt succeeded or failed?

The **Signons and Attempted Signons** report provides a history of all user sign-ins during a specified time period.

How do I find details about why authentication failed for a sign-in attempt?

In the **Signons and Attempted Signons** report, click the magnifying glass in the first column of the failed sign-in attempt. The **View System Account Signon** page displays the authentication policy components that applied to the sign-in attempt: **Matching Authentication Rule** and **Matching Authentication Type Restriction**.

The Forgot Password link on my sign in to Workday page is missing. How do I restore it?

To restore the **Forgot Password** link on your sign in to Workday page, verify these settings in your tenant:

1. On **Edit Tenant Setup - Security**, ensure that the **Enable Forgotten Password Reset** check box is selected.
2. On **Edit Tenant Setup - Notifications**, ensure that **Disable All Emails** isn't selected in the **General Email Notification Settings** section.

If the **Forgot Password** link is still missing from your sign in to Workday page, clear your browser cache.

Which authenticators and browsers does Workday support for Passwordless Sign-In authentication?

Workday supports these combinations of authenticators and browsers for passwordless sign-in authentication:

Operating System	Browsers	Authenticators
macOS	Google Chrome Microsoft Edge	Apple Touch ID YubiKey Nano YubiKey 5 NFC YubiKey 5Ci
Microsoft Windows	Google Chrome Microsoft Edge	Microsoft Windows Hello YubiKey Nano YubiKey 5 NFC YubiKey 5Ci

How do I know if my tenant is subject to virtual clean room (VCR) restrictions?

If you don't disable VCR restrictions for your tenant, Workday requires certain Workday implementers to sign in from a restricted set of Workday IP ranges. We provide information about the restriction on the:

- **Manage Authentication Policies** report.
- **Signons and Attempted Signons** report.

If an implementer can't sign in to Workday due to VCR restrictions, Workday identifies the failed sign-in attempt as from outside the authorized network range.

How can I ensure that implementers can access my Workday tenant if it's subject to VCR restrictions?

Define an authentication policy that specifically accommodates implementers that are subject to VCR restrictions, and those implementers that aren't:

- Create a rule that has *Any* selected under **Authentication Condition** for the All VCR Restricted Implementers security group. Place this rule at the top of the rule order.
- Create a rule that applies your desired IP restrictions to the All Non-VCR Restricted Implementers security group. Place this rule second in the rule order.
- (Optional) Create a rule that applies your desired IP restrictions to the Implementers security group. Place this rule after the other 2 rules in the rule order.

You can also set authentication type restrictions on the rules for implementers.

How can I disable VCR restrictions?

If your company security policy requires all implementers to access Workday from your company network, contact Workday Support about removing the VCR restrictions for your tenant.

Related Information
Tasks
Clearing Cache
Examples
Example: Virtual Clean Room (VCR) Restricted Implementer Access for IP-Restricted Tenants on page 94

Configurable Security

Configurable Security Basics

Setup Considerations: Configurable Security

You can use this topic to help make decisions when planning your use of configurable security. It explains:

- Why to set it up.
- How it fits into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What It Is

Workday configurable security enables you to control the items users can view and the actions they can perform in your tenant. You can determine how you want to group users through security groups. You can specify the items and actions that members of security groups can view and perform through security policies.

Business Benefits

- Automate permission assignments by grouping users based on similar attributes, saving you the effort of setting up permissions individually.
- Manage access to integrations, reports, mobile devices, and IT access using a single security model, making it easier to maintain access at scale.
- Make mass changes to your security configuration as your organization grows.

Use Cases

- Automatically add new users to a defined security group based on their position, such as adding financial analysts to a security group when hired.
- Enable users to access only nonsensitive portions of data, such as enabling HR administrators to access aggregated payroll results.
- Provide different levels of access for different types of users in the same tenant.

Questions to Consider

Questions	Considerations
How do you want to determine who can view items and perform actions in Workday?	Workday provides different types of security groups to enable you to address the security needs of your organization. Example: Job-based security groups

Questions	Considerations
	enable you to control access to items and actions by grouping users based on their job details. Workday groups similar items and actions into different security policies. While you can't change the items and actions secured to security policies, you can change the security groups associated with the security policies. By associating security groups with security policies, you can enable members of the security groups to access the secured items and actions.
What level of permission do you want to provide to tasks and reports?	Workday groups similar tasks and reports into security domains. To provide access to the tasks and reports, set View or Modify permission on the security policies that secure them. View permission provides users with access to only the tasks and reports that Workday designates with View access. Reports and reporting items are typically the items that Workday designates with View access. Modify permission provides users with access to all the tasks and reports secured to the domain.
What level of permission do you want to provide to business processes?	You can use business process security policies to set permissions for the actions on business processes, such as initiation and action steps. You can set different permissions for actions on business processes, such as View All, Rescind, and Deny permissions.
What's your change management strategy for security?	The changes you make to security policies go into effect when you activate the changes. You can: • Revert to earlier versions of your security configuration. • Prepare complex changes to your security before enabling the changes. While you can revert to earlier versions, Workday doesn't provide security policy change control to help you keep alternate valid configurations. When you revert to another configuration, the current configuration is no longer available.
Do third-party resources need access to your Workday tenant?	You can use Service Centers to grant third-party contracted organizations access to your Workday tenant without granting them access to sensitive data. Representatives from the third-party organizations have limited access to your Workday tenant and can support a subset of workers in your organization. The representatives aren't workers but can perform tasks in Workday within a

Questions	Considerations
	predefined scope. Example: Helping employees enroll in benefits or unlock their locked accounts.

Recommendations

Workday recommends that you exercise caution when making security modifications. You should thoroughly understand the impact of any configuration changes related to security modifications.

Before you create your own security groups, use Workday-provided, preconfigured security groups, which enable you to:

- Benefit from questions and feedback about the security groups as captured on Workday Community.
- Use Workday-verified security configurations.

Provide users with the fewest privileges to information and resources needed to accomplish their job functions. Providing users with the fewest privileges enhances the protection of your information and resources.

Turn off functional areas and security policies that you don't currently use to simplify your security configuration.

Review setup considerations for security groups and security policies for additional recommendations.

Requirements

To set permissions for domains and business processes, enable each functional area as well as its security policies. Enabling a functional area doesn’t automatically enable all the security policies within the functional area.

Review setup considerations for security groups and security policies for additional requirements.

Limitations

You can’t:

- Change the actions available on business process security policies.
- Change the items within domains.
- Create your own functional areas.
- Delete security policies.
- Move domains or business processes from 1 functional area to another.

When you revert to another configuration using security policy change control, the original configuration is no longer available.

Tenant Setup

No impact.

Security

These domains in the System functional area:

Domains	Considerations
Security Administration	Enables you to review and administer security. Provides the ability to view how Workday secures items.

Domains	Considerations
Security Configuration	Enables you to configure security and review your security configuration. Provides the ability to view and maintain functional areas, create security groups, and view security timestamps.

Business Processes

No impact.

Reporting

Reports	Considerations
Business Process Security Policies for Functional Area	Displays all business process security policies for a functional area.
Domain Security Policies for Functional Area	Displays all domain security policies for a functional area.
Functional Areas	Displays all functional areas and the domains and business processes in them.
Security Exception Audit	Displays errors and warnings involving your security configuration.
View Security for Securable Item	Displays how Workday secures delivered items.
View Security Group	Displays the associated security policies and configuration details for a security group.
View Security Groups for User	Displays the security groups that a user is a member of.

Integrations

No impact.

Connections and Touchpoints

Configurable security provides a comprehensive model for accessing items throughout Workday and on all devices.

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Related Information

Concepts

Concept: Configurable Security on page 112
Concept: Security Policy Change Control on page 204

Tasks

Maintain Security Group Permissions on page 129

Reference

Setup Considerations: Security Groups on page 122
Setup Considerations: Security Policies on page 195
Reference: Security-Related Reports on page 114
Reference: Security Group Types on page 133

Steps: Enable Functional Areas and Security Policies

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

Before you can configure security for workers in your tenant, enable the functional areas and security policies for secured items you want to provide access to.

Steps

1. Access the **Maintain Functional Areas** task.

   Select the **Enabled** check box for the functional areas you want to use.

   If a functional area doesn't display on the **Maintain Functional Areas** task, access the **Create Functional Area** task. You can specify the name of an existing domain group without a functional area to create the functional area.

   See Concept: Configurable Security.
2. Access the **Domain Security Policies for Functional Area** report.

   Select **Domain Security Policy** > **Enable** from the related actions menu of the domain security policy.

   Security: *Security Activation* domain in the System functional area.
3. Access the **Business Process Security Policies for Functional Area** report.

   Select **Business Process Policy** > **Edit** from the related actions menu of the business process type.

   Add security groups to relevant initiating actions. You can disable the business process security policy by removing all the security groups from relevant initiating actions.
4. Activate your changes to security policies.

   See Activate Pending Security Policy Changes on page 203.

Example

By enabling functional areas and security policies for:

- Activity streams, you can specify the workers who can collaborate with others.
- Extended enterprise learning, you can specify the workers who can create and manage extended enterprise learners.
- Lease accounting, you can specify the workers who can manage account posting rules.

Related Information
Reference
The Next Level: Functional Area Enablement

Steps: Set Up Security Permissions

Prerequisites

- Enable the functional areas for the items you want to use.
- Security: *Security Configuration* domain in the System functional area.

Context

Set up security for workers in your tenant so they can access tasks, reports, and other secured items in Workday. Workers gain access to items when you:

- Add workers to security groups or identify an existing security group that contains the workers.

- Associate the security groups with the security policies that secure the items.
- Activate your changes to the security policies.

You can add workers to security groups by either:

- Assigning users to security groups directly. Example: Using user-based security groups.
- Deriving membership based on information about users. Example: Their role assignments or job details.

Steps

1. Identify an existing security group that contains the users for whom you want to set permissions.

   You can also access the **Create Security Group** task to create a new security group.

   See Reference: Security Group Types on page 133 and Reference: Workday-Delivered Security Groups on page 136.
2. (Optional) Access the **View Security for Securable Item** report.

   Identify the security policies that secure specified items.
3. Add the security group to the security policies.

   See Edit Domain Security Policies on page 200 and Edit Business Process Security Policies on page 201.
4. Activate your changes to security policies.

   See Activate Pending Security Policy Changes on page 203.
5. Verify your security configuration.

   See Reference: Security-Related Reports on page 114.

Result

Workers in the specified security groups can access items that Workday secures to the associated security policies.

Example

Set up security to determine who can:

- Access specified hold reasons and whether those workers can override or update the corresponding student holds.
- Complete an electronic Form I-9.
- Create and modify headcount plans and view and analyze plan data.

Related Information
Reference
The Next Level: Getting to Know Configurable Security

Concept: Configurable Security

You can control the items users can view and the actions they can perform in your tenant with configurable security.

Functional Areas

Workday groups reports, tasks, and other items into different functional areas. Each functional area includes items that enable users to perform similar actions. Example: The Benefits functional area includes reports, tasks, and other items for managing benefits.

Each functional area includes:

- Domains, which include reports, tasks, instance sets, report fields, integration templates, web services, and data sources.

- Business process types, which include the steps for actions in business processes, such as initiation and action steps.

To view functional areas and the domains and business processes within them, access the **Functional Areas** report.

When you purchase additional SKUs for Workday, you can use the **Maintain Functional Areas** task to enable functional areas. You can then create and test configurations specific to each SKU.

Security Groups

Security groups are collections of users that you can use to grant access to secured items and business process steps. You can create custom security groups to serve security requirements beyond the security groups in your tenant. You can add workers to security groups by either:

- Assigning users to security groups directly.
- Deriving membership based on information about users, such as their roles or job details.

Security Policies

Security policies enable you to configure access to groups of items and individual business process actions. By associating security groups with security policies, you can enable members of the security groups to access the secured items and actions. You can't change the items in a domain or actions in a business process.

You can set:

- Get and Put permissions for integrations.
- View and Modify permissions for reports, tasks, and other items secured to domains.

You can also set various permissions for actions on business processes, such as View All, Rescind, and Deny permissions.

Inheritance in Domain Security Policies

Workday defines parent-child relationships so that child security policies inherit permissions from a parent security policy.

Example: The *Set Up: Accounting Rules* domain inherits permissions from the *Set Up: Financial Accounting* domain. These relationships can help you maintain and update permissions for many items at once.

You can:

- Identify whether a domain security policy inherits permissions by accessing the domain security policy on the **View Domain** report.
- Override inherited permissions when a child security policy needs different permissions.
- Return to the parent permissions using the **User Parent Permissions** option on the **View Domain Security Policy** report.

The items in a parent security policy include the items from the domain it secures and all the subdomains. The domain it secures might not have securable items of its own. Overriding permissions doesn’t affect the inheritance on any other child security policies.

Note: Upon breaking inheritance of a child policy, a new snapshot is created that shows the addition of any security groups included at the time of activating policy changes. The new snapshot treats all security groups as new additions to the policy, including groups defaulted in from the original parent and any security groups you add or remove from the newly disinherited child.

Inherent Permissions

Workday provides default access to certain securable items through inherent permissions. While you can remove security groups from some domain security policies, the security groups retain access to the securable items that Workday secures to the security policies.

Example: The Implementers security group has inherent permissions to the *User-Based Security Group Administration* domain security policy. Members of the Implementers security group have permanent access to items secured by the domain.

The **Inherent Permission** field on the **View Domain** report lists the security groups that have permanent access to a domain security policy.

Security Policy Change Control

Workday tracks the date and time of each change you make to your security. Workday evaluates your security based on a timestamp of all your changes since a specified date and time. You can activate:

- Pending changes and create a new timestamp.
- Previous timestamps to revert to earlier versions of your security.

Related Information
Concepts
Concept: Security Groups on page 129
Concept: Security Policies on page 201
Concept: Security Policy Change Control on page 204
Reference
The Next Level: Getting to Know Configurable Security

Reference: Security-Related Reports

Workday provides reports in these areas to help you manage security in your tenant:

- Security Groups
- Security Policies
- Domains and Business Processes
- Workers
- Security Audits

Security Groups

Report	Description	Prompts
Action Summary for Security Group	View the security policies associated with a specified security group. This report only identifies domains that secure one or more task.	**Security Group**
Business Process Types and Initiating Security Groups	View all business processes and the security groups that have permission to initiate them.	None
Compare Permissions of Two Security Groups	Compare the security policy permissions for 2 security groups.	**Security Group 1** **Security Group 2** **Include Disabled Domains/ Functional Areas** (Optional)

Report	Description	Prompts
Security Analysis for Security Groups	View the secured items associated with 1 or more specified security groups.	**Security Group** (Optional) **Include Disabled Domains/ Functional Areas** (Optional)
View Security Group	View 1 security group and the associated security policies and configuration details.	**Security Group**
View Security Groups	View 1 or more security groups and the associated security policies and configuration details.	**Include Disabled Domains/ Functional Areas** (Optional) **Include Inactive Security Groups** (Optional) **Security Group Type(s)** (Optional)
View Web Service Operations Security Groups	Identify the security groups that you need to be a member of to run a specified web service.	**Web Service**
Web Service Security Audit	View the security groups that can run web service tasks.	**Web Service Task to Select** (Optional)

Security Policies

Report	Description	Prompts
Business Process Security Policies Changed within Time Range	View changes to business process security policies in your tenant and view when and who changed the security policies.	**From** (Optional) **To** (Optional) **Include Changes to Security Groups** (Optional)
Business Process Security Policies for Functional Area	View all business process security policies for a functional area.	**Functional Area** **Business Process** (Optional)
Business Process Security Policies with Pending Changes	Review pending changes to business process security policies before activating them.	None
Business Process Security Policy History	Audit changes to specified business process security policies and view when and who changed the security policies.	**Business Process Type** (Optional) **From** (Optional) **To** (Optional)
Domain Security Policies Changed within Time Range	View changes to every domain security policy in your tenant and view when and who changed the security policies.	**From** (Optional) **To** (Optional) **Include Changes to Security Groups** (Optional)
Domain Security Policies for Functional Area	View all domain security policies for a functional area.	**Functional Area**

Report	Description	Prompts
Domain Security Policies with Pending Changes	Review pending changes to domain security policies before activating them.	None
Domain Security Policy History	Audit changes to specified domain security policies and view when and who changed the security policies.	**Domain Security Policy** **From** (Optional) **To** (Optional)
Domain Security Policy Summary	View the current security configuration for every domain in 1 or more functional areas.	**Functional Areas** (Optional)
Functional Areas	View all functional areas and the domains and business processes in them.	None
View Security for Securable Item	Identify how Workday secures specified delivered items.	**Securable Item**

Domains and Business Processes

Report	Description	Prompts
All Domains	View the functional areas, subdomains, and super domains for each domain in Workday.	None
Inactivated Domains	View all inactivated domains and the policy statuses.	None
Secured Items in Multiple Domains	View the delivered items that Workday secures to more than 1 domain.	None
View Domain	View the reports, tasks, and other items that Workday secures to a domain.	**Domain**

Workers

Report	Description	Prompts
Compare Security of Two Worker Accounts	Compare the security group assignments for 2 workers.	**Worker 1** **Worker 2**
Security Analysis for Landing Page Worklet	View whether a Workday account can access specified landing pages and the associated worklets.	**Landing Pages** **Account**
Security Analysis for Securable Item and Account	View the security policies and security groups that grant a Workday account access to a delivered item. You can also view a user's access restrictions, exclusion sets, and the security	**Securable Item** **Account** **Show Details** (Optional)

Report	Description	Prompts
	groups that determine access to securable items or accounts.	
Security Analysis for Workday Account	View the access permissions for 1 or more Workday accounts.	**Workday Account** (Optional) **Include Disabled Domains/ Functional Areas** (Optional)
Security History for User	View a detailed history of the transactions involving a Workday user.	**User** **From** (Optional) **To** (Optional)
Security History for Users Audit Report	View security events related to changes in users' user-based security group assignments. To access a full audit of all previous security events, you can generate the report without entering information in the starting prompts. When you populate the **Organizations** prompt, the report will generate members that were active as of the **To** end date.	**From** (Optional) **To** (Optional) **Users** (Optional) **Organizations** (Optional)
Test Security Group Membership	Evaluate whether a user is a member of a security group.	**Is User** **In Security Group** **for Target Instance** (Optional)
Test Security Rule	Evaluate whether a Workday account satisfies the conditions on a security rule.	**Security Rule** **Workday Account**
View Security Groups for User	View all the security groups that a user is a member of.	**Person**

Security Audits

Report	Description	Prompts
Security Exception Audit	Audit the details of errors and warnings involving security groups and security policies in your tenant.	None
Security Groups Not Referenced in any Security Policy	Audit the security groups that you aren't using on any security policy.	None
Security History	Audit the security changes for a specified organization.	**Organization** **From** (Optional) **To** (Optional)

Report	Description	Prompts
		Include Subordinate Organizations (Optional)
View All Security Timestamps	Audit all security timestamps, including current and previous timestamps, and the comments.	None

Related Information
Concepts
Concept: Configurable Security on page 112
Concept: Security Policies on page 201
Concept: Security Groups on page 129
Reference
Workday Community: Security Reports

FAQ: Configurable Security

What if users can access items that they shouldn't be able to access?

The **Security Analysis for Securable Item and Account** report can help you determine if you need to remove:

- A security group from a security policy.
- A user from a security group.

The report can also help you determine if a secured item displays in more than 1 domain. Users with different levels of access in different domains have the most permissive access granted. Example: A user has Modify permission to a secured item when the user has:

- View permission to the secured item in 1 domain.
- Modify permission to the secured item in another domain.

You can also use the **Access Restrictions That Apply to User** table in the report to confirm the

access restrictions, exclusion sets, and unrestricted security groups associated with a user's account.

If users have permission to access a secured item that they shouldn't be able to access:

- View the **Access Rights to Organizations** section in the security group definition and inheritance.
- Access the **Secured Items in Multiple Domains** report.

All changes to security groups or security policies are effective immediately. Before you make changes, consider how the changes affect other access for the security group and user.

What if users can't access items that they should be able to access?

These reports can help you compare the security groups for a user with the security groups on a securable item:

- **View Security for Securable Item**
- **View Security Groups for User**

Using the information from these reports:

- Add the user to a security group that has permission to access the item.
- Grant access to a security group that the user belongs to.

Before you change your tenant, consider:

- The user's access when you associate them with a security group that has permission to access the item.
- The number of other users in the security groups that the user is in.

How does a user get access to an instance?

A user can get access to an instance through a role-based security group. Access the **Security Analysis for Securable Item and Account** report to identify:

- The role-based security group that provides the user with access to the instance.
- The instance ID.

Using this information and the **Test Security Group Membership** report:

- Add 1 security group at a time to identify the security group that provides access.
- Identify the security groups assigned to the user or the role assignments for the user.

Which security groups have permission to view background processes?

You can view background processes in the **Background Processes for a Process** report.

Any user who belongs to an Administrative security group can view all background processes in this report.

All users can view the background processes for processes that they've run. For Integrations, users can view processes if you provide them with permission to view the relevant templates.

Users can view these background process types if they have the appropriate permissions:

- **Integration Processes**: Users must belong to an Administrative-type security group secured to the *Integration Build*, *Integration Debug*, or *Integration Event* security domains.
- **Report Processes**: Users must belong to an Administrative-type security group secured to the *Report Background Processes* security domain.
- **Scheduled Reports**: Users must belong to an Administrative-type security group secured to the *Scheduled Report Processes* security domain.

Which security groups have permission to access My Reports and download content from Workday?

Security groups that have access to the *Export to PDF and Excel* domain security policy can:

- Access the **My Reports** report.
- Download content from Workday to PDF or Microsoft Excel files.

By default, Workday configures the All Users security group on the *Export to PDF and Excel* domain security policy.

Security groups that have access to the domain security policy can download these types of content:

- Drill-down menus.
- Grids.
- Items accessed using context menus.
- Pages.

The domain security policy has no impact on self-service type content. Security groups that don't have access can download items such as:

- Business forms.
- Pay advice.
- W-2 forms.

(Workday Extend only) For Export to Excel grids, Workday doesn't support security policies configured on the *Export to PDF and Excel* domain. To prevent users from exporting grid data, the Workday Extend app developer must disable the Export to Excel feature on the grid.

How can I fix securable items that have exceptions?

Exceptions can occur when someone changes a security policy, which invalidates an access assignment. This happens when you activate a pending security policy change in which a:

- Business process security policy is missing a security group that the business process still uses.
- Security policy specifies a security group that you deleted from Workday.

Before you remove a security group from a business process security policy, remove the security group from the business process definition.

Access the **Security Exception Audit** report to:

- Identify problem areas.
- Remove the invalid security group from the security policy or business process definition.

When a business process starts, you can:

- Reassign the step routed to an invalid user.
- Rescind the process.

In either case, change the business process definition for that organization to specify only valid security groups.

Why does a user receive an error when attempting to access a task in My Tasks or an email notification link?

A user might receive an error when someone changes the security policy on a business process after the process starts.

The error might also occur when the security group with permission to access the step doesn't have either:

- **View All** access for events in progress.
- **View Completed Only** access for completed events.

To assess the business processes, access these reports:

- **Business Process Policy View Audit**: Identify security groups that don't have View access to components of business process types that might involve them.
- **Security Exception Audit**.

Where can I view the different role and security group assignments for 2 different workers?

Access the **Compare Security of Two Worker Accounts** report to view:

- Assignment differences for roles and security groups.
- Common assignments for 2 workers.

Where can I view the different security policy assignments for 2 different security groups?	Access the **Compare Permissions of Two Security Groups** report.
Where can I view the permissions granted to a security group?	Access the **View Security Group** report and view a security policy from 1 of these tabs: • **Business Process Permissions** tab for business process security policies. • **Security Permissions** tab for domain security policies. You can also access the **Action Summary for Security Group** report. You can use the report to view details about the security policy assignments for a security group.
Where can I view the security for securable items?	Access the **View Security for Securable Item** report.

Related Information
Reference
Workday 32 What's New Post: Configurable Security Reporting
Workday 32 What's New Post: View Security for Securable Item

Security Group Basics

Setup Considerations: Security Groups

You can use this topic to help make decisions when planning your configuration and use of security groups. It explains:

- Why to set them up.
- How they fit into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What They Are

Security groups are collections of users that you can use to grant access to secured items and business process steps. You can create custom security groups to serve security requirements beyond the security groups in your tenant. You can add workers to security groups by either:

- Assigning users to security groups directly.
- Deriving membership based on information about users, such as their roles or job details.

Business Benefits

Security groups save you time configuring and managing permissions for large collections of users.

Use Cases

Depending on the type of security group you use, you can:

- Enable credit card companies to integrate with Workday.
- Enable HR Partners to view worker data for their assigned organizations.
- Enable only contingent workers to complete time tracking.
- Enable third-party help desks to access target data.

Questions to Consider

Questions	Considerations
Do you want to set security permissions for individual users?	You can use user-based security groups to set security permissions for individual users, such as administrators with elevated privileges. Setting permissions for individual users can be maintenance intensive. When you want to automate maintenance, Workday recommends using other types of security groups, such as role-based or job-based security groups.
Do you want to enable third-party users to access secured items?	Service Center security groups enable third-party users in a Service Center to access secured items. You can use user-based security groups to provide certain users in the Service Center with elevated privileges.
Do you want to adjust the permissions on an existing security group without changing the security group?	Use these types of security groups to adjust permissions by combining members from other security groups: • Aggregation security groups. • Intersection security groups. Aggregation security groups include users who are members of at least 1 included security group. Example: Provide HR Partners and HR Executives with the same permissions. Intersection security groups include users who are common to all the included security groups. Example: Combine these security groups so HR Partners who are members of both security groups get access to secured content: • HR Partner security group based on supervisory organization. • HR Partner security group based on location hierarchy. The configuration enables you to separate permissions between HR Partners in England, Germany, and Ireland from HR Partners in the United States and Canada.
Do you want to set permissions based on a worker's job?	Job-based security groups enable you to automate security group assignments based on the job profile details of a worker. Example: Enable hourly, nonexempt workers to access time tracking functionality.

Questions	Considerations
	To change the members of a job-based security group, you can: • Change the job details that you reference in the security group definition. • Change the job details of the users you want to add or remove from the security group.
Do you want to set permissions to support a worker population in a certain location?	You can use constrained role-based security groups to provide access based on the position you assign to a role in a location hierarchy. Example: The manager of the Berlin office sits in the London office. You can enable the manager to access data in Germany by assigning the position on the Manager role for Berlin. You can use organization membership security groups to provide broad access using a location hierarchy. Because you're using a location hierarchy, Workday automatically updates permissions as locations change in the hierarchy. You can use location membership security groups to provide access based on a specific location. Example: Set permissions for workers in Austin, Texas.
Do you want to enable workers to access data for only their assigned organizations?	You can constrain certain security group types so that members can access only data that you secure to their organizations. You can also constrain role-based security groups by: • Customer. • Job requisition. • Prospect. • Requisition. • Supplier contract. You can use user-based security groups and other unconstrained security group types to grant access to secured content regardless of organization. Workday recommends using unconstrained security groups for: • Domains that enable you to modify configurations, such as *Set Up* domains. • Centralized teams that need tenant-wide access to all data, such as your Human Resources Information Services and Human Resources Information Technology teams.

Recommendations

Workday recommends that you:

- Avoid creating intersection security groups that contain only 1 security group.
- Avoid creating user-based security groups that contain only 1 user.

- Remove security groups from security policies when you intend to replace the security groups with aggregation, intersection, or segment-based security groups.
- Not select the optional **Inactive** check box to disable members' permissions when that security group is a member of, or administrator for, another security group. The same applies if security groups are already granted permissions to the *Security Configuration* domain.
- Test each change to a security group by signing in as other users and reviewing the data that the users can access.
- Use simple constraints when creating security groups to ensure that Workday evaluates security more quickly.

Many security policies have restrictions on the types of security groups that you can add to the security policies. Before you create security groups, consider the:

- Data points, tasks, reports, and business processes you want to provide access to.
- Security policies that secure those items.
- Types of security groups that you can associate with the security policies.

Use the default security groups in your tenant as a starting point for your configuration. You can then refine the security groups as you need to so you can:

- Take advantage of the questions that others ask on Workday Community by referencing the same security language.
- Use the security group configurations that Workday designs and verifies.

Consolidate similar business requirements into broad security groups. By configuring less-specific security groups, you can:

- Avoid activating many small security changes.
- More easily maintain security permissions.

The security groups you use can impact how quickly you can generate reports and route steps on business processes. When performance is an important consideration, use:

- Unconstrained role-based security groups.
- User-based security groups.

Copy security groups carefully to avoid providing new security groups with more access than you intend to provide. When you copy security groups, Workday copies all the security permissions to the new security group. When you want to change the permissions on the security group, you must remove security policies individually.

Requirements

No impact.

Limitations

When you configure intersection security groups, you can't use:

- Aggregation or other intersection security groups as exclusion criteria.
- Constrained security groups as exclusion criteria.
- Integration System and other intersection security groups as inclusion criteria.
- Intersection security groups in access restrictions.

You can't use these Workday-delivered security groups in intersection security groups:

- All Users
- Manager's Manager

Tenant Setup

No impact.

Security

These domains in the System functional area:

Domains	Considerations
Security Administration	Enables you to audit and administer security groups.
Security Configuration	Enables you to create and manage security groups.

You can use these delivered security groups to enable users to set and manage security in your tenant:

Security Groups	Considerations
Security Administrator	Can manage all security-related information regardless of organization.
Security Configurator	Can assign workers to security groups.
Security Partner	Can perform security management functions for assigned organizations.
System Auditor	Can audit security group setup.

Business Processes

No impact.

Reporting

These reports display security groups in your tenant and enable you to evaluate membership in the security groups:

Reports	Considerations
Action Summary for Security Group	Displays the security policies that you associate with a security group.
Compare Permissions of Two Security Groups	Displays the security policy permissions for 2 security groups.
Security Analysis for Security Groups	Displays the items that you associate with 1 or more security groups.
Test Security Group Membership	Displays whether a worker is a member of a security group.
View Security Group	Displays the configuration details and associated security policies for 1 security group.
View Security Groups	Displays the configuration details and associated security policies for 1 or more security groups.

You can also use the **Security Groups** data source to create custom reports about the security groups in your tenant. The data source displays 1 row for each security group and includes all security group types.

Integrations

No impact.

Connections and Touchpoints

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Related Information
Concepts
Concept: Security Groups on page 129
Setup Considerations: Security Policies on page 195
Reference
Reference: Security Group Types on page 133
Reference: Workday-Delivered Security Groups on page 136

Copy Security Group Permissions

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use the **Maintain Permissions for Security Group** task to:

- Easily migrate permissions across security groups of different types.
- Transition to new security models as your organization grows.

Using the task, you can copy permissions from an existing security group to:

- A new security group of the same type.
- An existing security group of the same or different type.

Steps

1. Access the **Maintain Permissions for Security Group** task.
2. Select *Copy* on the **Operation** field.
3. In the **Source Security Group** prompt, select an existing security group with permissions you want to copy.
4. In the **Target Security Group** prompt, select which security group you want to copy permissions to.
5. (Optional) If you're copying permissions between user-based security groups, you can select the **Copy User Assignments** check box to copy users from one security group to another.
6. On the **Domain Security Policy Permissions** tab, review the permissions on the source security group.

   You can select the check box on the **Selected** column to copy permissions to the target security group.

   To exclude permissions from the source security group:

   - Clear the check box on the **Selected** column, deleting the permission while displaying the row.
   - Select the **Remove Row** option, deleting the permission and row.

   Workday displays a selected box on the **From Source** column when permissions derive from the source security group.
7. Review business process security policy permissions from the source security group in the **Business Process Security Policy Permissions** tab. The tab displays when you copy permissions to a security group of the same type.

Result

Workday:

- Copies permissions to the target security group.
- Doesn't delete excluded permissions from the source security group.

Example

To prevent HR representatives from accessing compensation information about other HR representatives, you create an HR Partner intersection security group and assign relevant permissions. You later decide you want to use a rule-based security group instead. You can migrate the permissions from the intersection security group to the rule-based security group.

Next Steps

- Verify the changes to the target security group using the **View Security Group** task.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Concepts
Concept: Security Groups on page 129
Tasks
Activate Pending Security Policy Changes on page 203
Reference
2020R1 What's New Post: Mass Maintain Security Permissions

Delete Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can delete security groups that:

- You haven't activated, whether or not the security groups have members.
- You add to security policies, as long as you haven't activated the security policy changes.

You can't delete security groups that:

- You've added to security policies and activated the changes to.
- Are inactive.

The audit trail for security policies requires the retention of inactive security groups to function properly.

You can't restore deleted security groups.

Steps

1. Access the **Delete Security Group** task.
2. From the **Tenanted Security Group to Delete** prompt, select the security group you want to delete.
3. Select the **Confirm** check box.

Maintain Security Group Permissions

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use the **Maintain Permissions for Security Group** task to:

- Add and delete domain security policy permissions on an existing security group.
- Review business process security policy permissions on an existing security group.

Steps

1. Access the **Maintain Permissions for Security Group** task.
2. Select *Maintain* on the **Operation** field.
3. In the **Source Security Group** prompt, select an existing security group with permissions you want to change.
4. On the **Domain Security Policy Permissions** tab, review or delete domain security policy permissions.

   To delete permissions:

   - Clear the check box on the **Selected** column, deleting the permission while still displaying the row.
   - Select the **Remove Row** option, deleting the permission and row.
5. On the **Business Process Security Policy Permissions** tab, view business process security policy permissions on the source security group.

Next Steps

- Verify the changes to the target security group using the **View Security Group** task.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Concepts
Concept: Security Groups on page 129
Tasks
Activate Pending Security Policy Changes on page 203
Reference
2020R1 What's New Post: Mass Maintain Security Permissions

Concept: Security Groups

Security groups are collections of users that you can use to grant access to securable items in your Workday tenant. You can add users to security groups by either:

- Assigning users to security groups directly. Example: Using user-based security groups.
- Deriving membership based on information about users. Example: Their role assignments or job details.

Your tenant includes:

- Configurable security groups: Your implementation partner loads these commonly used security groups into your tenant during implementation. You can create, change, and delete these security groups.
- Workday-delivered security groups: Workday defines these security groups and determines their members. You can't create, change, or delete these security groups.

You can create your own security groups when your tenant doesn't include the ones you need.

Context Types

Workday enables you to restrict the access that members of a security group have using these context types:

- Unconstrained: Members can access all secured data instances.
- Constrained: Members can access a subset of secured data instances.
- Mixed: Members don’t have uniform access to secured data instances.

Mixed applies to these types of security groups:

- Aggregation
- Intersection

The name of a security group type can help you determine the access to secured data instances. Example: Members of role-based security groups (constrained) have contextual access.

Context Sensitivity

Constrained security groups provide members with access to a subset of secured data instances based on context. Example: Members have access to data in the context of their own organizations only. These types of security groups are context-sensitive by organization:

- Integration system (constrained).
- Job-based (constrained).
- Organization membership (constrained).
- Role-based (constrained).
- Service Center (constrained).

Role-based security groups (constrained) can also be context-sensitive by:

- Customer.
- Job requisition.
- Prospect.
- Requisition.
- Supplier contract.

These security groups become context-sensitive when they contain other groups that are context-sensitive:

- Aggregation
- Intersection
- Segment-based

Example: An intersection security group that contains a role-based security group (constrained) and a location membership security group is context-sensitive.

The organization type on the organization criteria must match the organization type on the security group restrictions on these security group types:

- Integration system (constrained).
- Intersection.
- Service Center (constrained).

Example: You can't add a security group to a security policy that you restrict to organization types other than Company when you:

- Include a role-based security group that is valid for security group restrictions of Roles – Company in the Intersection Criteria.
- Specify a Company in the Exclusion Criteria (Constrained Context) of an intersection security group.
- Specify a Company in the **Organizations** prompt of an integration system security group (constrained).

Workday grants securable item access to targets associated with a context-sensitive security group only when the targets and the item instance share the characteristic that makes the security group context-sensitive.

Example: An integration system security group is constrained from accessing certain web service tasks, based on its organization. A segment-based security group with access to an integration system security segment is context-sensitive by an integration system. You can't use the segment-based security group to grant integration systems to the constrained integration system security group. Instead, Workday recommends that you:

- Use an unconstrained security group with the segment-based security group.
- Don't grant the unconstrained security group access to any other domains.

Public Domains

Domain names that include the keyword Public provide access to public information, such as contact addresses. Access to these domains depends on the security group that you assign to the domains.

- Job-based security groups provide greater access to worker data profiles.
- Role-based security groups display the workers that a user supports.
- User-based security groups don't apply filters; administrators who require broad access typically use this type of security group.

Workday delivers job-based security groups that group members independently of the configuration of an organization. You can assign delivered job-based security groups to Worker Profile domains, such as:

- *All Contingent Workers*
- *All Employees*
- *All Users*

You can define your own security groups to meet your business needs. Examples: These security groups provide more open access to worker data:

- Job-based security groups, such as *All Managers*, with access to All Organizations enable any manager to access any worker.
- Job-based security groups for other groups, such as *Any HR Partner*. The security groups enable all HR Partners to access the information for any worker who you secure through a security policy.
- User-based security groups, when job-based security groups can't group users based on management levels or job profiles.

To secure the **Job Details** tab for workers with:

- Full data, place the security group you create on the *Worker Data: Public Worker Reports* domain in place of the Manager or HR Partner security groups.
- Limited data, place the security group you create on the *Worker Data: Current Staffing Information* and *Worker Data: General Staffing Information* domains.

Support Groups

Each worker is a member of 1 or more organizations. The other role assignees on those organizations make up the support groups for a worker. You can expose support groups for a worker on the **Support Groups** worklet using the **Configure Support Groups** task (secured to the *Set Up: Assignable Roles* domain).

Workers can use the worklet to view important contacts in their support groups, such as their HR Partner. The worklet displays specified security groups and the role assignees on those security groups.

Valid for Security Group Restrictions

The *Valid for Security Group Restrictions* field on the **View Security Groups for User** report identifies the security group types for a select security group. You can use the field, along with the restrictions on a security policy, to determine whether you can assign a security group to a security policy. Example: Workday uses the *Intersection Groups Containing Multiple Contextual Groups* type to indicate that an intersection security group contains more than 1 contextual security group.

Workday-Delivered Security Groups

You can't manually add or remove users or change the criteria that determines who is a member of a Workday-delivered security group. However, you can remove users from Workday-delivered security groups by changing the attributes of the users. Example: You can remove a manager from a Workday-delivered security group by moving them to an individual contributor role.

Related Information
Concepts
Concept: Configurable Security on page 112
Reference
Reference: Security-Related Reports on page 114
The Next Level: Getting to Know Configurable Security
The Next Level: Advanced Security: If You're Doing It Right, No One Will Know

Reference: Security Group Limitations

Consider these limitations in creating specific security groups:

Security Group Type	Limitations
Aggregation Security Groups	Aggregation security groups best function with groups that are quick to evaluate. You can't select groups that contain other security groups from the **Security Groups to Include** prompt: • Aggregation security groups. • Integration system security groups. • Rule-based security groups. You can only select these security group types from the **Security Group to Exclude** prompt: • Job-based security groups (unconstrained). • Location membership security groups. • Organization membership security groups (unconstrained). • Role-based security groups (unconstrained). • Service center security groups (unconstrained). • User-based security groups.
Intersection Security Groups	You can't select these security group types from the **Security Groups to Include** prompt: • Integration system security groups. • Intersection security groups. • Rule-based security groups.

Security Group Type	Limitations
	You can only select these security group types from the **Security Group to Exclude** prompt: • Job-based security groups (unconstrained). • Location membership security groups. • Organization membership security groups (unconstrained). • Role-based security groups (unconstrained). • Service center security groups. • User-based security groups. You can't select these organization types as an **Exclusion Criteria (Constrained Context)**: • Business Unit. • Payroll Company. • Union.
Rule-Based Security Groups	You can't select these security group types from the **Baseline Security Group** prompt: • Aggregation security groups. • Intersection security groups. • Rule-based security groups. • Segment-based security groups. You can select 1 membership security rule for each rule-based security group.
Segment-Based Security Groups	You can't select rule-based security groups from the **Security Groups** prompt.
User-Based Security Groups	You can only select other user-based security groups from the **Administered by Security Groups** prompt.

Related Information
Concepts
Setup Considerations: Security Groups on page 122
Concept: Security Groups on page 129

Reference: Security Group Types

Security Group Type	Description	Use Cases
Aggregation	Collection of users who are members of other security groups. Workday includes users who are members of any of the security groups used in the inclusion criteria. Workday excludes users who are members of a security group used in the exclusion criteria. Workday also excludes users	You can assign permissions to HR Partner (Supervisory Organization) and HR Partner (Location Membership) security groups through an HR Partner aggregation security group. You can use the HR Partner security group to assign permissions to both security groups simultaneously, making it

Security Group Type	Description	Use Cases
	who are members of a security group used in both the inclusion and exclusion criteria.	easier to maintain your security configuration.
Conditional role-based	Collection of users from constrained role-based security groups who satisfy a specified condition. You can constrain access based on a specified organization.	You can create a conditional role-based security group so you can enforce the Works Council regulations for team members located in Germany.
Integration system	Collection of 1 or more integration system users (ISUs) with access to web service tasks. You can constrain access based on a specified organization. When you specify organizations as inclusion or exclusion criteria for an integration system security group, match the organization type from the organization criteria to the security group restrictions.	You can enable a credit card company to integrate with Workday.
Intersection	Collection of users who are members of other security groups. Workday includes users who are members of all of the security groups used in the inclusion criteria. Workday excludes users who are in some or none of the security groups used in the inclusion criteria.	You can intersect a security group for U.S.-based workers with the Employee As Self security group. You can use the security group so only users in both the U.S. and the Employee As Self security groups can submit expense reports.
Job-based	Collection of users based on job details, such as: • Job category. • Job family. • Job profile. • Management level. You can constrain access based on a specified organization.	You can use the job profile of Chief Human Resources Officer (CHRO) to ensure that the person who fills the position automatically gets the correct access.
Level-based	Collection of users at 1 level in a hierarchy who can access data at another level in the hierarchy, independent of organization structures. You can group users based on these levels: • Compensation grade.	You can create a level-based security group so managers can view talent and performance information about their direct reports.

Security Group Type	Description	Use Cases
	• Management.	
Location membership	Collection of users who are in any of the included locations.	You can enable all workers in Tokyo to access target data.
Organization membership	Collection of users who are members of a specified organization type, such as: • Cost center. • Location hierarchy. • Pay group. You can constrain access to target data in the specified organization.	You can enable any worker in a Legal supervisory organization to be able to view all worker data in the tenant.
Prism access	Collection of users who are members of other unconstrained security groups. Workday includes users who are members of any of the security groups used in the inclusion criteria.	You can assign permissions to the Prism Data Administrator (User-based) security group through a Prism Data Admin - PASG prism access security group. You can use the Prism Data Admin - PASG security group to assign permissions to Prism-related domain security policies that don't allow permissions directly on unconstrained security groups.
Role-based	Collection of users associated with a specified assignable role. You can constrain access to the organizations that users support or lead.	You want to enable your support and leadership staff to access target data.
Rule-based	Collection of users who are members of a baseline security group and who satisfy a specified condition on the baseline security group.	You can enable only part-time workers to track their work hours by defining a security rule using the Time Type security field to identify part-time workers.
Segment-based	Collection of users who are members of other security groups. Provides access to components of a secured item. Members can be part of multiple groups and can have permission to access multiple security segments.	You can enable Benefits Administrators to be able to manage only benefits-related documents, without granting them the ability to manage payroll-related documents.
Service center	Collection of third-party users. Third-party users are users who aren’t workers in your organization charts and headcounts.	You can enable temporary workers to assist with the benefits enrollment process without hiring them through the typical staffing process.

Security Group Type	Description	Use Cases
	You can constrain access based on a specified organization.	
User-based	Collection of users by direct assignment. Users retain assignment regardless of job changes.	You can create a Bank Administrator user-based security group by directly assigning users to the security group. As you hire new employees to administer bank setup data, you can assign the employees to the security group directly.

Related Information
Concepts
Concept: Security Groups on page 129
Reference
Setup Considerations: Security Groups on page 122

Reference: Workday-Delivered Security Groups

Workday automatically populates these security groups. You can't create, edit, or delete membership to these groups. You can change what a group has access to by modifying domain or business process security policies. You can also update a user's attributes so that they're no longer a member of a Workday-delivered security group.

Example: To remove an employee from the Employee As Self security group, you could either terminate the worker or convert them to a contingent worker.

Security Group	Description
Academic Affiliate as Self	Includes users with an active academic appointment, which gives them access to self-service tasks.
Admissions Counselor as Self	Includes active student recruiters as determined by the status of these business processes: • *Activate Student Recruiter* • *Deactivate Student Recruiter*
All Academic Affiliates	Includes users with an active academic appointment as determined by the status of these business processes: • *Add Academic Appointment* • *End Academic Appointment*
All Admissions Counselors	Includes users with a completed *Admissions Counselor Event* business process event. Excludes users that you've offboarded with a completed *Admissions Counselor Off-Boarding Event* business process event unless you've reactivated them.
All Candidates	Includes users with a verified recruiting system account.

Security Group	Description
All Contingent Workers	Includes users with a completed *Contract Contingent Worker* event, where the contract start date is on or before today.
All Employees	Includes users with a completed *Hire* event, where the hire date is on or before today.
All External Committee Members	Includes users with: • A current committee membership as determined by the dates of the *Manage Committee Membership* business processes. • No other role in the tenant.
All Extended Enterprise Learners	Includes all users from outside your company who can access your learning catalog.
All External Learning Instructors	Includes all external, third-party instructors. External instructors can't: • Be extended enterprise learners. • Enroll in courses. • View worker profiles or details about a worker that aren't relevant to the courses that they teach.
All External Learning Users	Includes all users from outside your company who can access your learning catalog.
All External Students	Includes all external student users who can access your Career Site.
All Internal Learning Instructors	Includes all instructors that you created from workers already in your tenant who: • Give lessons. • Grade course work of learners. • Manage waitlists.
All Learning Assessors	Includes users who grade work, and record attendance in individual lessons or courses.
All Managers' Managers	Includes users with a manager role for a manager. Uses position-based evaluation logic to enhance security when a worker's direct manager: • Is on an international assignment. • Has multiple jobs in the enterprise.
All Non-VCR Restricted Implementers	Includes implementers who aren't subject to virtual clean room (VCR) sign-in restrictions as part of the implementer creation flow by the Engagement Manager.
All Pre-Contingent Workers	Includes users with a completed *Contract Contingent Worker* event, where the contract start date is after today.

Security Group	Description
All Pre-Employees	Includes users with a completed *Hire* event, where the hire date is after today.
All Project Members	Includes users assigned to a project: • Directly. • Indirectly through a resource or talent pool.
All Prospective Suppliers	Includes users with a prospective supplier account to an external supplier site.
All Recommenders	Includes users with a recommender account on an external student site. Workday automatically creates external student site accounts for recommenders when: • Student prospects submit applications with recommenders on an external student site. • Administrators add recommenders to applications submitted by student prospects on an external student site.
All Recruiting Agency Users	Includes users with a Recruiting Agency User account.
All Retirees	Includes users with a completed *Termination* event with the termination reason of Retirement.
All Service Center Representatives	Includes users with a Service Center Representative account.
All Students	Includes matriculated students as determined by the *Student Application Pre-Matriculation Event* business process.
All Student Prospects	Includes users with a Student Prospect account.
All Student Proxies	Includes users with student proxy accounts who have third-party permissions.
All Student Recruiters	Includes users with a Student Recruiting account.
All Supplier Prospect Group	Includes all public users who have access to set up external sites for external supplier system users.
All Terminees	Includes users with a completed *Termination* event, where the termination date is before today.
All Users	Includes users who can sign in to Workday, including Implementers and integration system users (ISUs).
All VCR Restricted Implementers	Includes implementers who are subject to virtual clean room (VCR) sign-in restrictions as part of the implementer creation flow by the Engagement Manager.
Any Organization Role (Leadership or Supporting)	Includes users with a role on an organization where the effective date is before today.

Security Group	Description
Award Contract Owner	Includes only the award contract owner on the award header. Enables award contract owners to report on just the awards that they own. Also used for routing the *Award Task Event* business process directly to the award contract owner for approval.
Candidate as Self	Includes users with a verified Recruiting System account, which gives them access to self-service tasks.
Candidate Notification Receiver	Includes users with a notification system account. Workday automatically creates notification system accounts for all candidates when you enable candidate fields in notifications.
Case Sharing	Includes users with shared access to nonconfidential cases, which enables them to view the shared case. These users can also add messages and internal notes to the shared case when you add this security group to these subdomains: • Help Case Messages • Help Case Internal **Note:** Workday automatically adds users to this security group when a case is shared with them. Similarly, Workday removes users from the security group when shared access is removed.
Case Solver Visibility	Includes case solvers who can access all nonconfidential cases that they created, regardless of the service team they're part of.
Commenter	Includes users with the Comment permission level for Drive items.
Constrained Proxy Users	Includes users who are given temporary access to securable items through constrained proxy.
Contingent Worker as Self	Includes users with a completed *Contract Contingent Worker* event, where the contract start date is on or before today. The security group provides users with self-service access to their own information.
Customer Contact As Self	Includes customer contacts with a Workday account, which gives them access to self-service tasks.
Editor	Includes users with the edit permission level for one or more Drive items, either from an individual sharing action or a group sharing action. This is a derived security group that Workday manages automatically. Example: If you enabled group sharing, and if a group contains all active users, sharing an item with that group causes Workday to add all active users into the Editor security group. These users have edit access only to the specific

Security Group	Description
	items that were shared with them. When a user no longer has edit permission access to any Drive items, Workday removes them from the Editor group.
Employee as Self	Includes users with a completed *Hire* event, where the hire date is on or before today. The security group provides users with self-service access to their own information.
Extended Enterprise Learner as Self	Includes all users from outside your company who can access your learning catalog. These users have a Workday account and can access self-service tasks.
External Learning Instructor as Self	Includes all external, third-party instructors with a Workday account who can access self-service tasks. External instructors can't: • Be extended enterprise learners. • Enroll in courses. • View worker profiles or details about a worker that aren't relevant to the courses they teach.
External Learning User as Self	Includes all external, third-party learners with a Workday account who can access self-service tasks.
External Committee Member as Self	Includes users with: • A current committee membership as determined by the dates of the *Manage Committee Membership* business processes. • No other role in the tenant. The security group provides users with self-service access to their own information.
External Compliance Site System	Includes all users with access to the external site for completing Section 2 of the Form I-9 for remote hire.
External Student as Self	Includes all external student users with access to non-worker career opportunities and self-service access to their own information.
External Supplier Site System	Includes anonymous users with access to information that's common for any prospective supplier accessing the external supplier registration site.
Implementers	Includes users created by Engagement Managers that implement customer tenants. On the 1st day of each month, Workday automatically deactivates implementer accounts that last logged in more than 180 days ago. This automated job disables all accounts but the wd-support, in IMPL, Preview, Prod, and Sandbox

Security Group	Description
	tenants. This job will not disable any implementer accounts created using Workday Central Login (WCL). Regularly deprovisioning implementer accounts enhances the security of both the *Implementers* security group and individual accounts across Workday. Due to the privileged nature of implementer accounts, you can't opt out of this security measure.
Inactive External Committee Members as Self	Includes users with a previous (not current) committee membership as determined by the dates of the *Manage Committee Membership* business processes. The security group provides self-service access to invitees for new committee memberships.
Initiator	Includes users who are members of a security group that's secured to at least 1 initiating action on a business process security policy. Example: All users who are part of the *Employee As Self* security group are included in the *Initiator* security group when *Employee As Self* is secured to at least 1 initiating action on any business process security policy. To view the members of the *Initiator* security group, view the security groups that can perform at least 1 initiating action on a business process security policy. Workday doesn't recommend: • Adding the *Initiator* security group to a domain security policy. Doing so grants access to all users to view all data. • Use the *Initiator* security group for routing notifications. Doing so can lead to notifications being sent to terminated employees' email addresses.
Internal Learning Instructor As Self	Includes all instructors that you created from workers already in your tenant who: • Give lessons. • Grade learners' course work. • Manage waitlists. This security group provides users with self-service access to their own information.
Learning Assessor as Self	Includes users who grade work, and record attendance in individual lessons or courses. The security group provides users with self-service access to their own information.
Matrix Manager (Supervisory Hierarchy Access)	Includes users with a matrix manager role for a matrix organization. You can secure the security group to grant members access to the supervisory reports of any managers within matrix

Security Group	Description
	organizations. This provides matrix managers with the visibility they need to support workers. For performance reasons, we recommend that you don't use this security group in business process action steps. Example: Helen is the matrix manager for the Matrix1 organization. Bob is a supervisory organization manager within Matrix1. Helen wants to see the business titles for all workers within Bob's supervisory organization. You assign the *Matrix Manager (Supervisory Hierarchy Access)* security group to the *Worker Data: Business Title on Worker Profile* domain. You give the group View access. Bob's supervisory organization includes subordinate organizations. Helen gains access to the workers in those organizations as well.
Manager for Majority of Event	Used only in employee reviews. Membership is derived by comparing a worker's manager at the start, midpoint, and end of an event. For employee reviews, the event time-span is the time-span of the review period. If the manager at the midpoint and the end of the event is the same, that manager is the Manager for Majority of Event. Otherwise, the manager at the start of the event is the Manager for Majority of Event. Workday also derives the Manager for Majority of Event for workers with multiple managers.
Manager's Manager	Includes users with a manager role for a manager. Uses position-based evaluation logic to enhance security when a worker's direct manager: • Is on an international assignment. • Has multiple jobs in the enterprise.
Mentor	Includes users with a proposed mentor for a mentorship event. When a mentorship event is approved, the user is the approved mentor for the mentorship.
Owner	Includes users with the Owner permission level for Drive items. After a user or administrator transfers ownership of an item, Drive removes the original owner from the Owner security group.
Pre-Contingent Worker as Self	Includes users with a completed *Contract Contingent Worker* event, where the contract start date is after today. The security group provides users with self-service access to their own information.
Pre-Employee as Self	Includes users with a completed *Hire* event, where the hire date is after today. The security group provides users with self-service access to their own information.

Security Group	Description
Primary Manager's Manager	Uses position-based evaluation logic to enhance security when a worker's direct manager: • Is on an international assignment. • Has multiple jobs in the enterprise.
Prism Dataset Editor	Includes users who have been granted Dataset Editor sharing permission on 1 or more Prism Analytics datasets.
Prism Dataset Owner	Includes users who have been granted Dataset Owner sharing permission on 1 or more Prism Analytics datasets.
Prism Dataset Viewer	Includes users who have been granted Dataset Viewer sharing permission on 1 or more Prism Analytics datasets.
Prism Delete Table Data	Includes users who have been granted Can Delete Table Data sharing permission on 1 or more Prism Analytics tables.
Prism Insert Table Data	Includes users who have been granted Can Insert Table Data sharing permission on 1 or more Prism Analytics tables.
Prism Select Table Data	Includes users who have been granted Can Select Table Data sharing permission on 1 or more Prism Analytics tables.
Prism Table Editor	Includes users who have been granted Table Editor sharing permission on 1 or more Prism Analytics tables.
Prism Table Owner	Includes users who have been granted Table Owner sharing permission on 1 or more Prism Analytics tables.
Prism Table Schema Editor	Includes users who have been granted Table Schema Editor sharing permission on 1 or more Prism Analytics tables.
Prism Table Schema Viewer	Includes users who have been granted Table Schema Viewer sharing permission on 1 or more Prism Analytics tables.
Prism Table Viewer	Includes users who have been granted Table Viewer sharing permission on 1 or more Prism Analytics tables.
Prism Truncate Table Data	Includes users who have been granted Can Truncate Table Data sharing permission on 1 or more Prism Analytics tables.
Prism Update Table Data	Includes users who have been granted Can Update Table Data sharing permission on 1 or more Prism Analytics tables.
Project Member as Self	Includes users assigned to a project, which gives them access to self-service tasks.

Security Group	Description
Prospective Supplier as Self	Includes users with a verified prospective supplier account, which gives them access to their supplier business entries.
Purchase Order Buyer	Includes users that create purchase orders or users that are specified in the Buyer field on a purchase order. You can remove a member from this security group by replacing the name on all purchase orders.
Recommender as Self	Includes users with a recommender account on an external student site. Workday automatically creates external student site accounts for recommenders when: • Student prospects submit applications with recommenders on an external student site. • Administrators add recommenders to applications that student prospects submitted on an external student site with at least 1 recommender. The security group provides users with self-service access to their own information.
Recruiting Agency User as Self	Includes recruiting agency users who can access the Workday security domains available for recruiting agency self-service.
Referee as Self	Includes users who have access to a unique URL where they can submit a reference for a candidate. This security group gives access to self-service tasks that enable referees to provide referral information.
Requisition Requester	Includes users who have created requisitions.
Requisition Sourcing Buyer	Includes users that are buyers for the company on a requisition and have access to these domains in the Procurement functional area: • Process: Sourcing - Goods • Process: Sourcing - Services
Retiree as Self	Includes terminated users with a termination reason of retirement, which gives them access to self-service tasks.
Role Maintainer	Includes users who can assign roles to organizations.
Seer	Includes users with the Seer permission level for Drive templates. The Seer permission level indicates that a template was distributed to the user but not shared with them.
Self Supplier Prospect Group	Includes users who have access to set up external supplier sites for external supplier system users.

Security Group	Description
Service Center Representative as Self	Includes users who have a Service Center Representative account, which gives them access to self-service tasks.
Sourcing Buyers for RFQ	Includes users that are buyers for the company on a request for quote and have access to these domains in the Procurement functional area: • Process: Sourcing - Goods • Process: Sourcing - Services
Student as Self	Includes matriculated students as determined by the *Student Application Pre-Matriculation Event* business process.
Student Prospect as Self	Includes users with a student prospect account, which gives them access to self-service tasks.
Student Proxy as Self	Includes users who act as student proxies to access student data based on third-party permissions provided by the student.
Supplier Contact as Self	Includes suppliers with a Workday account, which gives them access to self-service tasks.
Supplier Contract Specialist for Supplier Contract	Includes users whose names that you specify as the contract specialist on a supplier contract. You can remove a member from the security group by replacing the name on all supplier contracts.
Tax Filing Security Users	Includes users who can access other workers' citizenship status, date of birth, gender, ID, martial status, and worker profile information for tax filing purposes.
Terminee as Self	Includes terminated users who can still sign in to Workday, which gives them access to self-service tasks.
Viewer	Includes users with the view permission level for one or more Drive items, either from an individual sharing action, group sharing, or link sharing action. This is a derived security group that Workday manages automatically. Example: If you enabled group sharing, and if a group contains all active users, sharing an item with that group causes Workday to add all active users into the Viewer security group. These users have view access only to the specific items that were shared with them. When a user no longer has view permission access to any Drive items, Workday removes them from the Viewer group. Workday doesn't remove users from the Viewer group if both of these criteria apply: • You enabled link sharing in the **Edit Tenant Setup - System** task

Security Group	Description
	• The shared item was shared using the link sharing option
Worker Start Date Correction Assignee Group	Includes users who are setup to receive notifications for events that require manual action on the *Correct Worker Start Date* business process. The users also receive notifications when Workday encounters an issue for automatic actions on the business process. Don't add this group to any domain or business process security policy besides *Correct Worker Start Date*. Doing so can grant users access to a task or business process initiation.

Related Information
Concepts
Concept: Security Groups on page 129
Concept: Workday Central Login (WCL)

Example: Set Up Business Process Security for Workers with Multiple Positions

This example illustrates how to enable an HR partner to approve job changes for workers who have multiple positions.

Context

Sarah is a worker with these positions:

- A primary position for Company 1.
- A secondary position for Company 2.

You want to give the HR Partner for Company 1 the ability to approve *Change Job* business process events for Sarah.

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Steps

1. Access the **Create Security Group** task and enter:

Option	Description
Type of Tenanted Security Group	*Role-Based Security Group (Constrained)*
Name	*Primary HR Partner*

2. Click **OK**.
3. Specify these values:

Option	Description
Assignable Role	*HR Partner*
Access Rights to Organizations	*Applies To Current Organization And Unassigned Subordinates*
Access Rights to Multiple Job Workers	*Role has access to all positions*

4. Click **OK**.
5. Access the **Edit Business Process Security Policy** task and enter *Change Job*.
6. Click **OK**.
7. Add the new Primary HR Partner security group to the Approve action.
8. Click **OK**.
9. To activate your changes, access the **Activate Pending Security Policy Changes** task.
10. In the **Comment** field, enter Enable the HR partner to approve job changes for Sarah.
11. Select the **Confirm** check box.

Result

The security group enables the HR partner to approve job changes for Sarah.

Related Information

Tasks

Create Role-Based Security Groups on page 174

Example: Set Up Domain Security for Workers with Multiple Positions

This example illustrates how to expand domain security policies for workers who have multiple positions.

Context

Sarah is a worker with these positions:

- A primary position for Company 1 managed by Mark.
- A secondary position for Company 2 managed by Susan.

Jane is the global mobility partner for Company 2.

You want to give the managers and global mobility partner access to Sarah's compensation information.

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Steps

1. To create a Global Mobility Partner security group, access the **Create Security Group** task and enter:

Option	Description
Type of Tenanted Security Group	*Role-Based Security Group (Constrained)*
Name	*Global Mobility Partner*

2. Click **OK**.
3. Specify these values:

Option	Description
Assignable Role	*Manager*
Access Rights to Organizations	*Applies To Current Organization And Unassigned Subordinates*
Access Rights to Multiple Job Workers	*Role has access to all positions*

4. Click **OK**.

5. To create a Primary Manager security group, access the **Create Security Group** task and enter:

Option	Description
Type of Tenanted Security Group	*Role-Based Security Group (Constrained)*
Name	*Primary Manager*

6. Click **OK**.
7. Specify these values:

Option	Description
Assignable Role	*Manager*
Access Rights to Organizations	*Applies To Current Organization And Unassigned Subordinates*
Access Rights to Multiple Job Workers	*Role for primary job has access to all positions*

8. Click **OK**.
9. To change the Manager security group, access the **Edit Security Group** task.
10. Enter *Manager* from the **Tenanted Security Group** prompt and click **OK**.
11. Select **Role has access to the positions they support** in the **Access Rights to Multiple Job Workers** section.
12. Click **OK**.
13. To grant access to the new security groups, access the *Worker Data: Compensation by Organization* domain security policy.
14. Select **Domain** > **Edit Security Policy Permissions** from the related actions menu of the domain security policy.
15. In the **Report/Task Permissions** section, add *Global Mobility Partner* and *Primary Manager* with View access.
16. Click **OK**.
17. To activate your changes, access the **Activate Pending Security Policy Changes** task.
18. In the **Comment** field, enter Enable the managers and global mobility partner to access the compensation information for Sarah.
19. Select the **Confirm** check box.

Result

The security groups enable the managers and global mobility partner to access the compensation information for Sarah.

- Jane can access compensation information for both of Sarah's positions through the Global Mobility Partner security group.
- Mark can access compensation information for both of Sarah's positions through the Primary Manager security group.
- Susan can access compensation information for Sarah's secondary position through the changes to the Manager security group.

Related Information

Tasks

Create Role-Based Security Groups on page 174

Security Groups

Aggregation Security Groups

Create Aggregation Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use aggregation security groups to combine members from other security groups. Workday includes users who are members of at least 1 of the included security groups. You can also exclude workers who are members of a specified security group. Consider using aggregation security groups to ease maintenance when several security groups have common access requirements.

Steps

1. Access the **Create Security Group** task.
2. From the **Security Groups to Include** prompt, select 1 or more security groups whose members you want to include.
3. (Optional) From the **Security Group to Exclude** prompt, select a security group whose members you want to exclude.

   Workday excludes a user from an aggregation security group when the user is a member of:

   - A security group that you include.
   - Another security group that you exclude.

Example

You assign security permissions to the HR Partner (Supervisory Organization) and HR Partner (Location Membership) groups separately. As a result, you need to maintain those assignments individually. Alternatively, you can create an HR Partner aggregation security group that includes both the HR Partner (Supervisory Organization) and HR Partner (Location Membership) security groups. Using the aggregation security group in security policies, you can assign permissions to both security groups simultaneously, making it easier to maintain your security configuration.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Tasks
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203
Examples
Example: Create a Service Center Security Group for Benefits Support on page 188

Example: Set Up Expense Item Segment Access with Aggregation Security Groups

This example illustrates a way to enable only specific levels of employees to access expense items.

Context

You want to enable members of Corporate Affairs to access certain travel expenses. You use an organization-based security group to first define the pool of employees from Corporate Affairs. You then use a segment-based security group to grant them access to travel-related expense segments. You also create an aggregation security group that regularly evaluates member access.

Steps

1. Access the **Maintain Organization Types** report.
   a. On the **Custom** tab, click **Edit**.
   b. Add a row in the grid with these values:

Option	Value
Organization Type Name	Enter *Special Access - Business Unit*.
Allow Reorganization Tasks	Select the check box.
Show in Change Organization Assignments and Job Requisition	Select the check box.

   c. Click **OK** and **Done**.

   Security: *Set Up: Organization* in the Organizations and Roles functional area.
2. Access the **Maintain Organization Subtypes** task.
   a. Add a row in the grid with these values:

Option	Value
Organization Subtype Name	Enter *Special Access - Hidden*.
Organization Type	Select *Special Access - Business Unit*.

   b. Click **OK** and **Done**.

   Security: *Committee Definition: Set Up* in the Organizations and Roles functional area.
3. Access the **Create Custom Organization** task.
   a.

Option	Value
Custom Organization Type	Select *Special Access - Business Unit*.
Reorganization	*Create Reorganization*
Reorganization Name	*Special Access Organization Requirement*
Reorganization Date	Enter current date.

   b. Click **OK** twice.
   c.

Option	Value
Name	*Corporate Affairs*.
Subtype	*Special Access - Hidden*
Visibility	*Everyone*

   d. Click **OK**.

   Security: *Create: Custom Organization* in the Organizations and Roles functional area.

4. Access the **Create Membership Rule** task.
   a. In the **Rule Name** field, enter *Corporate Affairs* .
   b. From the **Job Families** prompt, select *MK-Product Marketing* and *Sales-Management*.
   c. Click **OK** and **Done**.

   Security: *Manage: Membership Rule Create* in the Organizations and Roles functional area.
5. Access the **View Custom Organization** report.
   a. From the **Custom Organization** prompt, select *Corporate Affairs* .
   b. Click **OK**.
   c. From the related actions menu of the organization, select **Reorganization** > **Assign Workers**.
   d. From the **Reorganization** prompt, select *Special Access Organization Requirement*.
   e. Click **OK**.
   f. From the **Select Members by Rules** prompt, select *Corporate Affairs* .
   g. Click **OK** and **Done**.

   Security: *Manage: Custom Organization* in the Organizations and Roles functional area.
6. Access the **Create Security Group** task.
   a. From the **Type of Tenanted Security Group** prompt, select *Organization Membership Security Group (Unconstrained)*.
   b. In the **Name** field, enter *Corporate Affairs*.
   c. Click **OK**.
   d. From the **Organizations** prompt, select *Corporate Affairs* .
   e. Select **Applies To Current Organization And All Subordinates**.
   f. Click **OK** and **Done**.

   Security: *Security Configuration* in the System functional area.
7. Access the **Create Expense Item Security Segment** task.
   a. In the **Name** field, enter *Travel Expenses*.
   b. From the **Expense Item** prompt, select *International Airfare*, *Meals w/Guests*, and *Private Accommodations*.
   c. Click **OK** and **Done**.

   Security: *Set Up: Expense Item Security Segments* in the System functional area.
8. Access the **Create Security Group** task.
   a. From the **Type of Tenanted Security Group** prompt, select *Segment-Based Security Group*.
   b. In the **Name** field, enter *Travel Expenses*.
   c. Click **OK**.
   d. From the **Security Groups** prompt, select *Corporate Affairs*.
   e. From the **Access to Segments** prompt, select *Travel Expenses*.
   f. Click **OK** and **Done**.

   Security: *Security Configuration* domain in the System functional area.
9. Access the **Create Security Group** task.
   a. From the **Type of Tenanted Security Group** prompt, select *Aggregation Security Group*.
   b. In the **Name** field, enter *Corporate Affairs - Travel Expenses*.
   c. Click **OK**.
   d. From the **Security Groups to Include** prompt, select *Travel Expenses*.
   e. Click **OK** and **Done**.

10. Access the **Maintain Permissions for Security Group** task.
    a. From the **Source Security Group** prompt, select *Corporate Affairs*.
    b. Click **OK**.
    c. Add a row in the **Domain Security Policy Permissions** grid with these values:

Option	Value
View/Modify Access	Select *View and Modify*.
Domain Security Policy	Select *Access Expense Item (Segmented)*.

    d. Click **OK** and **Done**.
11. Access the **Activate Pending Security Policy Changes** task.
    a. In the **Comment** field, enter *Enable Corporate Affairs to access expense item segments.*.
    b. Click **OK**.
    c. Select the **Confirm** check box.
    d. Click **OK**.

    Security: *Security Activation* in the System functional area.

Next Steps

Next, verify that members of Corporate Affairs can access and submit travel expense segments in an expense report.

Related Information
Tasks
Create Segment-Based Security Groups on page 185
Create Aggregation Security Groups on page 149

Conditional Role-Based Security Groups

Create Conditional Role-Based Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use conditional role-based security groups to apply a constrained role-based security group based on a condition. You can also use conditional role-based security groups to limit the display of detail-level data while still displaying aggregate values in these report types:

- Advanced reports, when you also select the **Summarize Detail Rows** check box on the report definition.
- Composite reports.
- Matrix reports.
- Trending reports.

In these report types, aggregate values reflect the **Security Group When Condition Not Met** evaluation. Detail-level data, such as in a drill-down menu, reflects the full security group evaluation.

Steps

1. Access the **Create Security Group** task.

2. As you complete the task, consider:

Option	Description
Condition	Location hierarchies to use as criteria for selecting which constrained role-based security group to apply.
Security Group when Condition Met	The constrained role-based security group to apply if the worker is in a specified location hierarchy.
Security Group when Condition Not Met and for Aggregate Data in Standard and Custom Reports	The constrained role-based security group to apply if the worker isn't in any specified location hierarchies.

Example

Your company headquarters are in the U.S. with branch offices in France and Germany. To comply with Works Council regulations for organizations, managers in Germany can only view worker data down to 2 levels in the organization chart. The regulations don't apply to offices in the U.S. and France. You can create a conditional role-based security group so you can enforce the Works Council regulations for team members located in Germany.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Tasks
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203
Examples
Example: Create a Conditional Role-Based Security Group on page 153

Example: Create a Conditional Role-Based Security Group

This example illustrates how to use a conditional role-based security group to apply a constrained role-based security group based on a specified condition.

Context

Your company headquarters are in the USA with branch offices in France and Germany. To comply with Works Council regulations for organizations, managers in Germany can only view worker data down to 2 levels in the organization chart. The regulations don't apply to offices in France and the USA.

You want to ensure that Workday:

- Enforces the Works Council regulations for team members in Germany.
- Includes workers who transfer to Germany from France or the USA.

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Steps

1. Access the **Create Security Group** task.
2. Enter these values:

Field	Enter
Type of Tenanted Security Group	*Role-Based Security Group (Constrained)*
Name	*Manager 2-Level*

3. Click **OK**.
4. In the **Assignable Role** prompt, select *Manager*.
5. In the **Access Rights to Organizations** section, specify:

Field	Enter
Access Rights to Organizations	*Applies to Current Organization and Subordinates to Level*
Subordinate Levels	*2*

6. In the **Access Rights to Multiple Job Workers** section, select *Role has access to the positions they support*.
7. Click **OK**.
8. Click **Done**.
9. Access the **Create Security Group** task.
10. Enter these values:

Field	Enter
Type of Tenanted Security Group	*Conditional Role-Based Security Group*
Name	*Conditional Management Chain - Germany*

11. Click **OK**.
12. In the **Location Hierarchy** prompt, select *2.2 Germany*.
13. In the **Role-Based Security Group (Constrained)** prompt of the **Security Group when Condition Met** section, select *Manager 2-Level*.
14. In the **Role-Based Security Group (Constrained)** prompt of the **Security Group when Condition Not Met and for Aggregate Data in Standard and Custom Reports** section, select *Management Chain*.
15. Click **OK**.
16. Click **Done**.

Result

Managers in the France office can view data for workers in France up to 3 levels down the organization chart. If a worker relocates to the Germany office, the managers won't be able to view data for the worker.

Next Steps

Add the conditional role-based security group to a domain security policy that controls access to worker data. Ensure that the constrained role-based security group isn’t on that domain security policy.

Related Information
Tasks
Create Conditional Role-Based Security Groups on page 152

Integration Security Groups

Create Integration System Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

Integration system security groups (ISSG):

- Include 1 or more integration system user (ISU) accounts.
- Provide Get and Put access to web service tasks.

When you create:

- Constrained ISSGs, you can filter data results contextually based on specified organizations such as supervisory organizations, cost centers, or location hierarchies. Example: Export data only for workers who are members of a specific supervisory organization.
- Unconstrained ISSGs, Workday provides members with access to data for all organizations.

When you constrain the security group type, filtering depends on the data access method:

- Public web services: Workday filters by element, not by row, based on the security of the web service operation. Example: A Workday integration that returns worker data only returns 1 row for each worker, but can filter out some worker data. Workday filters out data if different domains secure the element from the underlying web service operation and the web service operation.
- Reports as a Service: Workday filters by row based on the security of the report data source.

To interact with data in Workday, your integration system requires access to the web service operations that retrieve and insert the related data.

Steps

1. Access the **Create Security Group** task.
2. From the **Integration System Users** prompt, select ISUs to include in the security group.
3. (Constrained only) From the **Organizations** prompt, select organizations to which you want to constrain the security group.
4. (Constrained only) As you complete the **Access Rights to Organization** section, select organizations that the group criteria applies to:

Option	Description
Access to Current Organization Only	ISUs can access protected data for members of the specified organization.
Access to Current Organization And All Subordinates	ISUs can access protected data for members of the specified organization and all its subordinate organizations.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Tasks
Edit Domain Security Policies on page 200

Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203
Change Organization Visibility
Reference
Workday Community: API Documentation

Intersection Security Groups

Create Intersection Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use intersection security groups to combine members and constraints from other security groups. Workday includes workers and constraints that are common to all the included security groups. Workday excludes users and constraints in some or none of the included security groups. You can also explicitly exclude workers and constraints from a specified security group.

You can use intersection security groups to:

- Hide populations or target instances. Example: Hide data about HR employees from other HR employees.
- Intersect constrained role-based security groups that you enable for different organizations. Example: Intersect Canadian Workers with the Sales Organization.
- Limit self-service tasks or functionality to a certain population. Example: Limit time tracking to contingent workers.

Note: Workday doesn't recommend using intersection security for Compensation because it doesn't apply to all situations. One case where Workday can't evaluate intersection security is exclusion criteria, which depend on organizations. Many compensation components, including plans, grades, and pay ranges aren't associated with organizations. Managers can't have security over compensation components through organizations and roles the way they can for employees.

Steps

1. Access the **Create Security Group** task.
2. As you complete the **Intersection Criteria** section, consider:

Option	Description
Security Groups to Include	Workday includes users who are members of all selected security groups.
Security Group to Exclude	(Optional) Workday excludes users who are members of the selected security group.

   Note: You can only exclude unconstrained security groups from an intersection security group.
3. (Optional) In the **Exclusion Criteria (Constrained Context)** section, select 1 or more organizations to exclude target positions from.

   As you complete the section, consider:

Option	Description
Applies to Current Organization Only	Prevent users in the intersection security group from being able to access information about

Option	Description
	users with current positions in the selected organizations.
Applies to Current Organization And All Subordinates	Prevent users in the intersection security group from being able to access information about users with current positions in: • The selected organizations. • Any subordinate organizations.

Example

You want to enable only U.S.-based workers to submit expense reports in Workday. You can create an unconstrained organization membership security group for the U.S. Location Hierarchy that includes all U.S.-based workers. You can then intersect the security group with the Employee As Self security group. You can replace the existing self-service security groups on the *Self Service: Expense Report* domain with your new intersection security group. As a result, only users in both the U.S. Location Hierarchy and Employee As Self security groups can submit expense reports in Workday.

Note: Ensure that you remove security groups from their security policies when you replace them with an intersection security group.

Next Steps

When using intersection security groups, especially ones with exclusion criteria, Workday recommends that you test access, prompting, routing, and other functionality to ensure that security works as you expect.

To provide security permissions:

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Concepts
Concept: Intersection Security Groups on page 157
Tasks
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Concept: Intersection Security Groups

An intersection security group comprises 1 or more security groups. It includes users who are in all of the security groups.

Security Groups You Can Include

You can include these security group types in intersection security groups:

- Job-Based.
- Level-Based.
- Location Membership.
- Organization Membership.
- Role-Based.
- Segment-Based.

- Service Center.
- User-Based.
- Workday-Delivered, except for All Users and Manager's Manager.

Organization Types You Can't Exclude

You can't select these organization types as an **Exclusion Criteria (Constrained Context)**:

- Academic Unit or Academic Unit Hierarchy.
- Business Unit or Business Unit Hierarchy.
- Fund or Fund Hierarchy.
- Gift or Gift Hierarchy.
- Grant or Grant Hierarchy.
- Program or Program Hierarchy.
- Project or Project Hierarchy.
- Union.

You can access the **Security Exception Audit** report to find intersection security groups that include any of the organization types.

Recommendations

Workday recommends against using:

- Intersection security groups that use excluded organizations in business process security policies.
- Organization membership security groups that use custom organizations with dynamic membership rules in intersection security groups.

When working with such intersection security groups, test your configuration to make sure it works as intended.

Using Intersection Security Groups to Restrict Access

You can use intersection security groups to restrict access for:

- Students protected by the Family Educational Rights and Privacy Act (FERPA).
- Workers in sensitive positions.

You can restrict access by selecting a custom organization containing the workers or students from the **Exclude Target Position in Organization** prompt. If a worker or student held prior positions in other organizations, you can exclude the positions by adding them to the exclusion criteria.

You can’t create an intersection security group that:

- Includes a constrained role-based security group.
- Excludes another constrained role-based security group.

To configure a role-based security group without access to a given population:

- Select the role-based security group from the **Security Groups to Include** prompt.
- Select the population they can't access from the **Exclude Target Position in Organization** prompt.

Example: To prevent HR Partners from viewing other HR Partners, create a custom organization of HR Partners and:

- Select the HR Partner role-based security group from the **Security Groups to Include** prompt.
- Select the HR Partner custom organization from the **Exclude Target Position in Organization** prompt.

Additional Considerations

You can’t apply intersection security groups that intersect 2 or more context-sensitive security groups to:

- Processing actions on business processes.
- Security domains.

The restriction prevents you from applying security groups to policies for items that run with 1 contextual filter.

You can't add an intersection security group to a security policy that Workday restricts to organization types other than Company when you:

- Include a role-based security group that's valid for security group restrictions of Roles - Company from the **Intersection Criteria** prompt.
- Select a Company from the **Exclusion Criteria (Constrained Context)** prompt of an intersection security group.

Related Information
Tasks
Create Intersection Security Groups on page 156

Example: Configure Intersection Security Groups for Location-Based Restrictions

This example illustrates 1 way to use intersection security groups to exclude a subset managers from viewing compensation data in specific locations.

Context

You want to prevent a subset of managers from accessing compensation data for workers in Germany who aren't their direct reports. You use location membership and constrained role-based security to create an intersection group that excludes the managers from particular locales. You then assign permissions to the intersection security group to ensure that managers can't access pay information for workers in Germany.

Prerequisites

Security:

- *Security Activation* domain in the System functional area.
- *Security Configuration* domain in the System functional area.

Steps

1. Access the **Create Security Group** task.
   a. Select *Location Membership Security Group* from the **Type of Tenanted Security Group** prompt.
   b. In the **Name** field, enter *Workers - Germany*.
   c. Click **OK**.
   d. Select *TRANS Germany* from the **Locations** prompt.
   e. Click **OK** and **Done**.
2. Access the **Create Security Group** task.
   a. Select *Role-Based Security Group (Constrained)* from the **Type of Tenanted Security Group** prompt.
   b. In the **Name** field, enter *Manager (By Location)*.
   c. Click **OK**.
   d. Enter these values:

Option	Value
Assignable Role	*Manager*
Access Rights to Organizations	*Applies to Current Organization and Subordinates to Level*

Option	Value
Subordinate Levels	*2*

e. Click **OK** and **Done**.

3. Access the **Create Security Group** task.
   a. Select *Intersection Security Group* from the **Type of Tenanted Security Group** prompt.
   b. Enter *Germany - Compensation Data* in the **Name** field.
   c. Click **OK**.
   d. On the **Edit Intersection Security Group** task in the **Intersection Criteria** section, select *Manager (By Location)* from the **Security Groups to Include** prompt.
   e. In the **Security Groups to Exclude** section, select *Workers - Germany*.
   f. Click **OK** and **Done**.

Next Steps

Add the intersection security group to security policies and activate pending security policy changes.

Related Information
Tasks
Activate Pending Security Policy Changes on page 203
Create Intersection Security Groups on page 156
Create Location Membership Security Groups on page 168
Edit Domain Security Policies on page 200
Reference
The Next Level: The Basics of Intersection Security

Example: Create an Intersection Security Group That Excludes a Target Population

This example illustrates 1 way to use role-based security to limit access information about a target population of workers.

Context

You want to enable recruiters to view job application data for all workers apart from members of the executive management team. You can use role-based security to create an intersection security group that excludes the target population. You can then assign appropriate permissions to the recruiters in the intersection security group.

Prerequisites

Security:

- *Security Activation* domain in the System functional area.
- *Security Configuration* domain in the System functional area.
- *Set Up: Assignable Roles* domain in the Organizations and Roles functional area.

Steps

1. Access the **Maintain Organization Types** report.
   a. On the **Custom** tab, click **Edit**.
   b. Add a row on the grid.
   c. Enter these values:

Option	Value
Organization Type Name	Enter *Special Access - Executive Management*.
Allow Reorganization Tasks	Select the check box.
Show in Change Organization Assignments and Job Requisition	Select the check box.

   d. Click **OK** and **Done**.
2. Access the **Maintain Organization Subtypes** task.
   a. Add a row on the grid.
   b. Enter these values:

Option	Value
Organization Subtype Name	Enter *Special Access - Hidden*.
Organization Type	Select *Special Access - Executive Management*.

   c. Click **OK** and **Done**.
3. Access the **Create Custom Organization** task.
   a. Select *Special Access - Executive Management* from the **Custom Organization Type** prompt.
   b. Select *Create Reorganization* from the **Reorganization** prompt.
   c. Enter *Special Access Organization Requirement* in the **Reorganization Name** field.
   d. Set the **Reorganization Date** to the current date.
   e. Click **OK** twice.
   f. Enter *Executive Management* in the **Name** field.
   g. Select *Special Access Hidden* from the **Subtype** prompt.
   h. Select *Everyone* from the **Visibility** prompt.
   i. Click **OK**.
4. Access the **Create Membership Rule** task.
   a. Enter *Executive Management* in the **Rule Name** field.
   b. Select *Executive Management* from the **Job Families** prompt.
   c. Click **OK** and **Done**.
5. Access the **View Custom Organization** report.
   a. Select *Executive Management* from the **Custom Organization** prompt.
   b. Click **OK**.
   c. From the related actions menu of the organization, select **Reorganization** > **Assign Workers**.
   d. Select *Special Access Organization Requirement* from the **Reorganization** prompt.
   e. Click **OK**.
   f. Select *Executive Management* from the **Select Members by Rules** prompt.
   g. Click **OK** and **Done**.

6. Access the **Maintain Assignable Roles** task.
   a. Add a row on the grid.
   b. Enter these values:

Option	Value
Role Name	Enter *Recruiters (By Supervisory).*
Enabled for	Select *Supervisory*.
Is Leader/Is Supporting	Select **Is Supporting**.

   c. Click **OK** and **Done**.
7. Access the **Create Security Group** task.
   a. Select *Role-Based Security Group (Constrained)* from the **Type of Tenanted Security Group** prompt.
   b. Enter *Recruiters (By Supervisory)* in the **Name** field.
   c. Click **OK**.
   d. Select *Recruiters (By Supervisory)* from the **Assignable Role** prompt in the Group Criteria section on the **Edit Role-Based Security Group (Constrained)** task.
   e. Select the **Applies To Current Organization And Unassigned Subordinates** button in the **Access Rights to Organizations** section.
   f. Select the **Role has access to the positions they support** button in the **Access Rights to Multiple Job Workers** section.
   g. Click **OK** and **Done**.

   Note: Remove recruiters from their individual security policies before you add them to an intersection security group.
8. Access the **Create Security Group** task.
   a. Select *Intersection Security Group* from the **Type of Tenanted Security Group** prompt.
   b. Enter *Recruiters* in the **Name** field.
   c. Click **OK**.
   d. In the **Intersection Criteria** section on the **Edit Intersection Security Group** task, Select *Recruiters (By Supervisory)* from the **Security Groups to Include** prompt.
   e. Make these selections in the **Exclusion Criteria (Constrained Context)** section:

Option	Value
Exclude Target Position in Organization	Select *Executive Management*.
Applies to Current Organization and All Subordinates	Select.

   f. Click **OK** and **Done**.
9. Access the **Maintain Permissions for Security Group** task.
   a. Select *Recruiters* from the **Source Security Group** prompt.
   b. Click **OK**.
   c. Add a row on the **Domain Security Policy Permissions** grid.
   d. Enter these values:

Option	Value
View/Modify Access	Select *View Only*.
Domain Security Policy	Select *Candidate Data: Job Application*.

   e. Click **OK** and **Done**.

10. Access the **Activate Pending Security Policy Changes** task.

a. Enter *Enabling Recruiters to view job application data for all workers except for members of Executive Management* in the **Comment** field.
b. Click **OK**.
c. Select the **Confirm** check box.
d. Click **OK**.

Result

Recruiters can view hiring data for every worker except executive management.

Related Information

Concepts

Concept: Intersection Security Groups on page 157

Example: Excluding HR Partners from Intersection Security Groups

This example illustrates 1 way to exclude users from role-based security groups using intersection security.

Context

As a security administrator, you want to prevent HR Partners from viewing compensation data about other HR Partners. You first create a custom role and organization for partners who will have limited access to other partners' data. You use a constrained role-based security group to exclude users from the HR Partners security group. You then create an intersection security group so you can exclude HR Partners from viewing compensation data of the same role.

Prerequisites

Security:

- *Security Activation* domain in the System functional area.
- *Security Configuration* domain in the System functional area.

Steps

1. Access the **Maintain Assignable Roles** task to create the role of *Custom Org Partner*. This enables you to create a custom organization in which HR Partners have limited access to other partners' information.

See Set Up Assignable Roles

2. Access the **Create Custom Organization** task.

a. Select *New Custom Org* for the **Custom Organization Type**.
b. From the **Reorganization** type, select *Create Reorganization*.
c. Enter *HR Partner Reorg.* for the **Reorganization Name**.
d. Enter the current date for the **Reorganization Date**.
e. Click **OK** twice.
f. Enter these values:

Option	Value
Name	*HR Partner (Reorg)*.
Subtype	*Department*.
Visibility	*Role Assignees and Members*.
Role	*Custom Org Partner*.

Option	Value
Assigned To	*HR Partner* or equivalent.

g. Click **OK**.

Note: Workday doesn't recommend using dynamic rules to assign members to custom organizations.

3. Access the **Create Security Group** task.
   a. From the **Type of Tenanted Security Group** prompt, select *Role-Based Security Group (Constrained)*.
   b. Enter *HR Partners (Excluding Users)* for the **Name**.
   c. Enter these values:

Option	Value
Group Criteria	*HR Partner* for the **Assignable Role**.
Access Rights to Organizations	*Current Organization and All Subordinate Organizations*.

   d. Click **OK** and **Done**.
4. Access the **Create Security Group** task.
   a. From the **Type of Tenanted Security Group** prompt, select *Intersection Security Group*.
   b. Enter *HR Partners (Compensation Access)* in the **Name** field.
   c. From the **Security Groups to Include** prompt, select the *HR Partner* constrained role-based security group.
5. Select an organization that contains the population you want to exclude from the **Exclude Target Position in Organization** prompt.
   a. Enter these values:

Option	Value
Security Groups to Include	*HR Partners (Excluding Users)*.
Exclude Target Position in Organization	*HR Partner (Reorg)*.
Applies to Current Organization And All Subordinates	Select.

   b. Click **OK** and **Done**.

Note: Workday doesn't recommend using intersection security groups that use excluded organizations in business process security policies. When working with such intersection security groups, test your configuration to make sure it works as intended.

Next Steps

Add the intersection security group to security policies and activate pending security policy changes.

Related Information

Tasks

Activate Pending Security Policy Changes on page 203
Create Intersection Security Groups on page 156
Create Role-Based Security Groups on page 174
Edit Domain Security Policies on page 200

Reference

The Next Level: The Basics of Intersection Security

Job-Based Security Groups

Create Job-Based Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use job-based security groups to set security permissions based on job details. You can create:

- Constrained job-based security groups so members of the security group can access instances for select organizations.
- Unconstrained job-based security groups so members of the security group can access instances for all organizations.

When you create constrained job-based security groups, you can define membership based on these job details:

- Job category.
- Job family.
- Job profile.
- Management level.

When you create unconstrained job-based security groups, you can also define membership based on these job details:

- Exempt jobs.
- Nonexempt jobs.
- Work shift.

Steps

1. Access the **Create Security Group** task.
2. In the **Group Criteria** section, select the job details you want to associate with the security group.
3. (Constrained only) In the **Access Rights** section, select access rights for the security group.

   The organization type from the organization criteria must match the organization type from the security group restrictions. Example: When you select Company, you can add the security group to only security policies restricted to the Company organization type.
4. (Constrained only) As you complete the section, consider:

Option	Description
Applies to Current Organization Only	Workers with the specified job details can access securable items for specified organizations.
Applies to Current Organization And All Subordinates	Workers with the specified job details can access securable items for specified organizations and all subordinate organizations. Example: You select this option when you create a job-based security group (constrained) based on the: • Senior Vice President job profile. • Supervisory organization type. To determine who has permission to access worker information, Workday ascends the

Option	Description
	supervisory organization hierarchy of the worker to find someone with the Senior Vice President job profile.

Example

Security Group Type	Example
Job-based security group (unconstrained)	You want to enable the Chief Human Resources Officer (CHRO) of your company to view actual values for benchmarking. You can configure an unconstrained job-based security group to ensure that the person who fills this position in your organization automatically gets the correct access. When you create the unconstrained job-based security group, you can use the job profile of CHRO as the criteria for membership. As a result, Workday automatically updates the security assignment as different individuals move in and out of the CHRO position.
Job-based security group (constrained)	You want to enable workers in a Team Lead job profile to have access to other workers in their supervisory organization. You don't want them to have access to workers outside of their own supervisory organization. You can create a constrained job-based security group using the Team Lead job profile as the criteria for the group. You can then grant the access to the Supervisory Organization type and apply that access to only the current organization.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Tasks
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Example: Create Security Groups for an Organizational Hierarchy

This example illustrates 1 way to identify levels in an organizational hierarchy.

Context

You want to route expense approvals above a certain value to people in your organization at VP or higher levels. You create a constrained job-based security group limited to members of the organization who are at VP or higher levels in the supervisory hierarchy. You then create an intersection security group to ensure that only members of the job-based security group and supervisory hierarchy can approve expenses.

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Steps

1. Access the **Create Security Group** task.
   a. From the **Type of Tenanted Security Group** prompt, select *Job-Based Security Group (Constrained)*.
   b. In the **Name** field, enter *Expense Approval*.
   c. Click **OK**.
   d. In the **Group Criteria** and **Access Rights** sections, make these selections:

Option	Value
Job Profile	Select *Vice President*.
Apply to Organization Type	Select *Supervisory* and *Apply to Current Organization and All Subordinates*.

   e. Click **OK** and **Done**.
2. Access the **Create Security Group** task again.
   a. From the **Type of Tenanted Security Group** prompt, select *Intersection Security Group*.
   b. In the **Name** field, enter *High-Value Expense Approval*.
   c. In the **Group Criteria** and **Access Rights** sections, make these selections:

Option	Value
Security Groups to Include	Select *Expense Approval* and *Management Chain*.
Exclusion Criteria (Constrained Context)	Select *None of the Above*.

   d. Click **OK** and **Done**.

Next Steps

Add the intersection security group to a domain security policy that controls the visibility and approval of high-value expenses. Next, submit a high-value expense item as a worker and verify that a VP or higher member can see (and approve) it.

Related Information
Tasks
Create Job-Based Security Groups on page 165
Create Intersection Security Groups on page 156
Maintain Security Group Permissions on page 129

Level-Based Security Groups

Create Level-Based Security Groups

Prerequisites

Complete the:

- **Create Management Level Hierarchy** task to create management hierarchies.
- **Maintain Compensation Grade Hierarchy** task to create compensation hierarchies.

Security: *Security Configuration* domain in the System functional area.

Context

Level-based security groups define how workers at 1 level can access worker data at another level, independent of organizational structures. Level-based security groups associate with these types of leveled structures:

- Compensation grade hierarchies: Workday maps workers to each level based on their compensation grade.
- Management-level hierarchies: Workday maps workers to each level based on their job profile.

You can use level-based security groups with Workday Talent Management functionality, such as nBox reporting and Find Workers. Workday doesn't recommend you use level-based security groups on security policies in other application areas.

Steps

1. Access the **Create Security Group** task.
2. In the **Group Criteria** section, specify some or all levels of workers in a hierarchy that can access securable items.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Tasks
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Membership Security Groups

Create Location Membership Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

Location membership security groups enable you to group workers who are in any of the specified locations. The security group type isn't context-sensitive. That is, Workday doesn't match worker location to the location of the secured item.

Steps

1. Access the **Create Security Group** task.
2. From the **Locations** prompt, select the locations of the workers you want to include in the security group.

Example

Example: You want to restrict HR Partners from viewing application information for workers who live in Japan. You create a location membership security group for workers in Japan. You then create an intersection security group using a constrained role-based security group of HR Partners (By Location), excluding workers in the location membership security group.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Create Organization Membership Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use organization membership security groups to set security permissions for workers in specified organizations. You can include organizations of any type, such as Company or Cost Center. You can also include workers in subordinate organizations. When you create:

- Constrained organization membership security groups, Workday matches the organization for a worker to the organization for secured items.
- Unconstrained organization membership security groups, Workday provides a subset of workers with access to securable items when they belong to any included organization.

Steps

1. Access the **Create Security Group** task.
2. Select organizations with workers you want to include in the security group. When you create:
   - Constrained security groups, select 1 organization.
   - Unconstrained security groups, select 1 or more organizations.
3. (Constrained only) As you complete the task, consider:

Option	Description
Applies to Current Organization Only	Workers can access securable items for specified organizations.
Applies to Current Organization And All Subordinates	Workers can access securable items for specified organizations and all subordinate organizations.

Example

Security Group Type	Example
Organization membership security group (unconstrained)	You want any worker in a Legal supervisory organization to be able to view all worker data in the tenant. You can create an unconstrained organization membership security group that references the Legal supervisory organization. You can then apply the security group to the necessary security policies.
Organization membership security group (constrained)	You want any worker in a cost center hierarchy to be able to view other workers in their cost center hierarchy. You don't want them to be able to view workers outside of the cost center hierarchy. You can create a constrained organization membership security group that references the cost center

Security Group Type	Example
	hierarchy. You can then apply the security group to the necessary security policies.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information

Tasks

Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Prism Access Security Groups

Create Prism Access Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use Prism access security groups to combine members from other Prism access security groups. Workday includes users who are members of at least 1 of the included security groups. Use Prism access security groups to assign permissions to users in an unconstrained security group in Prism-related domain security policies. Some Prism-related domains allow Prism access security groups instead of unconstrained security groups.

Steps

1. Access the **Create Security Group** task.
2. From the **Unconstrained Security Groups** prompt, select 1 or more unconstrained security groups whose members you want to include.

Example

You want to give unconstrained access to a group of workers who can create and edit Prism Analytics tables. You can create a user-based security group that includes the workers. You can then create a Prism access security group that includes the user-based security group. You can then edit the security policy for the Prism Tables: Create domain, and assign permissions to the Prism access security group.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information

Tasks

Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Steps: Set Up Tenant for Prism Analytics

Role-Based Security Groups

Setup Considerations: Role-Based Security Groups

You can use this topic to help make decisions when planning your configuration and use of role-based security groups. It explains:

- Why to set them up.
- How they fit into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What They Are

With role-based security groups, you can control access to items and actions based on roles you create and assign to members of your organizations. You can assign roles to positions or jobs. You can also constrain the security group type to certain areas of an organization that each position or job supports.

Business Benefits

Using role-based security groups, you can assign and remove access rights automatically as workers change positions or jobs, enabling you to:

- Derive membership instead of explicitly defining it.
- Reduce the number of security groups to maintain.

Use Cases

Role-based security groups enable you to automatically:

- Add new HR representatives to an HR Partner role-based security group instead of having to assign them to the security group manually.
- Remove permissions when an engineer takes on a new position.

Questions to Consider

Questions	Considerations
How do you provide access to only specific instances of secured data?	You can use: • Conditional role-based security groups to constrain access based on location hierarchies. Example: Managers in Germany can have permission to access more levels in an organization than managers in the United States. • Constrained role-based security groups to constrain access based on organizations and other role-enabled objects. Example: Recruiters can only access job applications for their organizations.

Questions	Considerations
How do you configure role-based security groups for optimal performance?	The security groups you use can impact how quickly you can generate reports and route steps on business processes. To optimize performance: • Avoid filling a role using an organization assigned through a membership rule. • Avoid layers of intersecting role-based security groups. • Use unconstrained role-based security groups. When you configure constrained role-based security groups, you can improve performance by setting the access rights to the current organization and all subordinate organizations.
How does your staffing model affect role-based security groups?	The staffing model you use can impact whether workers backfill vacancies and inherit the associated permissions. With the: • Job management staffing model, Workday closes vacancies. When you hire a new worker, you must create a new job. The new worker doesn't inherit the original role assignments. • Position management staffing model, vacant positions remain open. New workers can backfill the vacant positions and inherit the original role assignments.
How do you provide similar permissions to multiple roles?	Workday recommends that you use aggregation security groups to set similar permissions. When you copy security groups, you must manually update permissions on each security group separately during security changes. Example: Your organization has HR Partner and HR Executive roles. You can add these roles to role-based security groups and add the security groups to an HR Management aggregation security group. When HR Executive and HR Partner need: • Different permissions, use the HR Executive or HR Partner security group to define the unique permissions. • Similar permissions, use the aggregation security group to define the common permissions.

Recommendations

Use:

- 1 role for each role-based security group to simplify your security configuration.
- 1 organization type for each role, except when you use hierarchical organizations that roll up to other organizations. Example: You can use 1 role for Cost Center Hierarchy and Cost Center because they're part of the same organization type.

- Unconstrained role-based security groups carefully. Anyone with the position you associate with the role can access the secured data for all organizations.
- User-based security groups to provide specific users, such as administrators, with access to securable items that aren't organization-specific.

Before you create role-based security groups, review the:

- Data points and business process steps you want to provide access to.
- Security policies that secure those items.
- Types of security groups that you can associate with the security policies.

Use consistent naming conventions for roles. Examples:

- HR Partner describes the HR functional area with modify access; HR Analyst describes the area with view access for HR data.
- Finance Partner describes the Financial functional area with modify access; Finance Analyst describes the area with view access for financial data.

Requirements

No impact.

Limitations

No impact.

Tenant Setup

No impact.

Security

Domains	Considerations
Security Administration domain in the System functional area.	Enables you to manage who can assign role permissions.
Security Configuration domain in the System functional area.	Enables you to create, view, and delete role-based security groups.
Manage: Organization Roles domain in the Organizations and Roles functional area.	Enables you to run audits and reports on roles.
Set Up: Assignable Roles domain in the Organizations and Roles functional area.	Enables you to view and maintain roles.

Business Processes

No impact.

Reporting

Reports	Considerations
Role Assignment Permissions	Displays the security groups that can administer each role in your tenant.
Role Assignments for Worker Position	Displays the roles and the associated role-based security groups for a specified worker.

Reports	Considerations
Roles for Organization and Subordinates	Displays the hierarchy of a specified organization.
Unassigned Roles Audit	Displays unassigned roles in your tenant.
Unfilled Assigned Roles Audit	Displays assigned roles with positions or jobs that no workers fill.
View Assignable Roles	Displays all roles in your tenant and the security groups that can assign the roles.
View Security Groups	Displays existing role-based security groups.
Worker Roles Audit	Displays the roles for each worker within a specified organization.

Integrations

No impact.

Connections and Touchpoints

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Related Information
Concepts
Concept: Assign Roles
Concept: Roles, Time Zones, and Snapshots
Concept: Security Groups on page 129
Concept: Staffing Models
Reference
Setup Considerations: Roles
Reference: Security Group Types on page 133

Create Role-Based Security Groups

Prerequisites

- Create assignable roles to use on the security group.
- Security: *Security Configuration* domain in the System functional area.

Context

You can use role-based security groups to derive security permissions based on roles. Role assignments involve assigning a role to a given worker position or job for a specified organization or role-enabled instance. When you create:

- Constrained role-based security groups, you can constrain access based on organizations or other role-enabled objects. Example: Recruiters can only access job applications for their organizations rather than for all organizations in your tenant.
- Unconstrained role-based security groups, you can provide access to all instance data in all organizations. Example: Recruiters can access job applications for all organizations in your tenant.

Steps

1. Access the **Create Security Group** task.

2. (Constrained only) In the **Access Rights to Organizations** section, select the access rights for the security group. The section relates solely to the security access associated with the role assignment.

   As you complete the section, consider:

Option	Description
Applies to Current Organization Only	Workers with the specified role can access securable items for the current organization. Example: Caitlin has the Compensation Partner role in the Operations organization. When you select this option, Caitlin can access data for workers in the specified organization only.
Applies To Current Organization And Unassigned Subordinates	Workers with the specified role can access securable items for the current organization and all subordinate organizations that don't have the specified assignable role. Example: Caitlin has the Compensation Partner role in the Operations organization. Robert has the role in the Facilities Group subordinate organization. Caitlin can access data for workers in all subordinate organizations, except data for workers in the Facilities Group subordinate organization.
Applies to Current Organization And All Subordinates	Workers with the specified role can access securable items for the current organization and all subordinate organizations. Example: Caitlin has the Compensation Partner role in the Operations organization. Robert has the role in the Facilities Group subordinate organization. Caitlin can access data for workers in all subordinate organizations, including data for workers in the Facilities Group subordinate organization.
Applies to Current Organization and Subordinates to Level	Workers with the specified role can access securable items for the current organization and all subordinate organizations. The subordinate organizations are up to a specified number of levels under the specified organization. You can use the **Subordinate Levels** field to specify the number of levels under the organization in the hierarchy. Example: Caitlin has the Compensation Partner role in the Operations organization. Robert has the role in the Facilities Group subordinate organization, which is 1 level below the Operations organization. Caitlin can access data for workers in subordinate organizations that are 1 level below the specified organization when you: • Select this option.

Option	Description
	• Specify 1 on the **Subordinate Levels** field.

Note: When you view the organization, Workday displays security access on the **Security Groups** tab, not on the **Roles** tab. Workers automatically inherit roles from the top-level organization down through the hierarchy. When **Inherited** displays in the **Role From** column on the **Roles** tab, the worker has access to the organization only when you also assign the worker to the security group displayed on the **Security Groups** tab.

3. (Constrained only) In the **Access Rights to Multiple Job Workers** section, select permissions to position or job data, and person data, for workers with multiple jobs:

Option	Description
Role has access to the positions they support	Grants access only for the job or position that you assign to the role in the specified organization. Example: Sarah has a primary position at Company 1 that Mark manages and a secondary position at Company 2 that Susan manages. When you select this option: • Mark can access Sarah's person data and primary position data for Company 1. • Susan can access Sarah's person data and secondary position data for Company 2.
Role for primary job has access to all positions	Grants access to assignees who have a role in the organization associated with the primary job or position. Denies access to assignees who have a role in the organization associated with an additional job or position. Example: Sarah has a primary position at Company 1 that Mark manages and a secondary position at Company 2 that Susan manages. When you select this option, only Mark can access Sarah's: • Person data. • Primary position data for Company 1. • Secondary position data for Company 2.
Role has access to all positions	Grants access to assignees who have a role in the organization associated with the primary or additional job or position. Example: Sarah has a primary position at Company 1 that Mark manages and a secondary position at Company 2 that Susan manages. When you select this option, both Mark and Susan can access Sarah's: • Person data. • Primary position data for Company 1. • Secondary position data for Company 2.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information

Tasks

Edit Domain Security Policies on page 200

Edit Business Process Security Policies on page 201

Activate Pending Security Policy Changes on page 203

Reference

Setup Considerations: Role-Based Security Groups on page 171

Examples

Example: Set Up Domain Security for Workers with Multiple Positions on page 147

Example: Set Up Business Process Security for Workers with Multiple Positions on page 146

Concept: Role-Based Security Groups (Constrained)

With role-based security groups, you can control access to items and actions based on roles you create and assign to members of your organizations. For workers, you assign roles to positions. For nonworkers, you assign roles directly to the:

- Academic Affiliate.
- Service Center Representative.
- Student Recruiter.

Constrained role-based security groups are context-sensitive because Workday matches security group members to the role-enabled object of an item. Only members with a role on the role-enabled object can access securable items in a domain.

Organization Assignments

Workday determines the organization to which a particular instance of a secured item belongs. Workday only grants access to workers in positions or roles that support that organization. Example: You can use a constrained role-based security group to ensure that only a worker with the HR Partner role can review or approve a step in the *Hire* business process.

Access to Subordinate Organizations

You can restrict access to subordinate organizations that are a specified number of levels below the current organization in a hierarchy. Access rights to organization data that you grant to a constrained role-based security group dictate whether workers can access subordinate organizations. If you don't assign anyone to a role in an organization, Workday searches up the hierarchy until it finds a role with access rights.

Reorganizations

When you create constrained role-based security groups, you can decide whether you want subordinate organizations to inherit the permissions from a role-enabled object. Workday recommends that you re-evaluate your configuration during reorganizations if you configure a constrained role-based security groups so unassigned subordinate organization inherit permissions from a parent organization. Otherwise, subordinate organizations might not have the appropriate role assignments after the reorganization goes into effect.

Example: Logan manages Adam in Payroll. Logan hires Betty to manage Adam and has Betty report to Logan. When Betty begins to manage Adam, Logan loses access to data about Adam. Logan loses access

because Adam is in a subordinate organization that inherits permissions from a parent organization. Because Betty is in the parent organization to Adam, Betty gains access to data about Adam.

Rule-Based Security Groups

Create Rule-Based Security Groups

Prerequisites

Create a security rule.

Security: *Security Configuration* domain in the System functional area.

Context

You can use rule-based security groups to constrain the members on a baseline security group using conditional rules. Examples: You can enable:

- Employees on leave to have self-service access.
- Employees from separate countries to be able to use self-service expense reporting functionality.
- Managers who have active contingent workers in their departments to share reports on contingent workers.
- Only nonexempt US employees to clock in and out.

With rule-based security groups, you can:

- Modify rule criteria without needing to activate individual security policy changes.
- Reuse rule criteria in multiple rule-based security groups.
- Use conditional rules to restrict recruiters' access to instances in which they are an applicant to a job requisition.
- Use conditional rules that aren’t maintenance intensive.

Steps

1. Access the **Create Security Group** task.
2. Select a security group with members you want to modify from the **Baseline Security Group** prompt.
3. As you complete the **Membership** section, consider:

Option	Description
Include Members by Rule	Include members from the baseline security group who match the criteria on the security rule.
Exclude Members by Rule	Exclude members from the baseline security group who match the criteria on the security rule.

Example

You want to enable only part-time workers to track their work hours in Workday. You can define a security rule using the Time Type security field to identify part-time workers. You can then apply the security rule on the inclusion criteria of a rule-based security group. As the baseline security group, you can use the All Users security group. By adding the new security group to the *Worker Data: Time Tracking* domain, you can enable only part-time workers to track their work hours.

Next Steps

After configuring the security group:

- Add the security group to security policies.

- Activate pending security policy changes.
- When you associate a security group with security policies, replace the existing security group with your new security group.
- When you want to enable the permissions on an inactive security group, activate the security group.

Use the **Test Security Group Membership** report to evaluate whether a Workday account is a member of a rule-based security group. An account isn't a member when the account either:

- Doesn't match the business object on the security rule.
- Doesn't satisfy at least 1 condition in a security rule on the inclusion criteria.
- Satisfies all the conditions in a security rule on the exclusion criteria.

Related Information

Tasks

Edit Domain Security Policies on page 200

Edit Business Process Security Policies on page 201

Activate Pending Security Policy Changes on page 203

Reference

Feature Release Note: Rule-Based Security Framework

FAQ: Rule-Based Security Groups on page 183

Examples

Example: Set Up Rule-Based Security Groups on page 182

Create Security Rules

Prerequisites

- Enable any additional report fields that you want to specify in your security rule conditions, using the **Maintain Fields for Security Rules** task.
- Security: *Set Up: Security Rules* domain in the System functional area.

Context

You can configure security rules to define criteria for determining membership on rule-based security groups. You can only use security rules on rule-based security groups.

Steps

1. Access the **Create Security Rule** task.
2. Select a business object from the **Business Object** prompt.

   You can only select 1 business object on a security rule.
3. (Optional) Specify a security rule that includes conditions you want to copy from the **Copy Condition from Rule** prompt.
4. Specify the rule criteria from the **Rule Conditions** grid.

   You can include up to 5 rule conditions on each security rule.

Next Steps

Add the security rule to rule-based security groups.

Use the **Test Security Rule** report to evaluate whether a Workday account satisfies the conditions on a security rule. You can't specify a security rule on the report when the security rule contains report fields secured to self-service domains.

Related Information
Reference
FAQ: Rule-Based Security Groups on page 183
Feature Release Note: Rule-Based Security Framework
Examples
Example: Set Up Rule-Based Security Groups on page 182

Enable Report Fields for Rule-Based Security

Prerequisites

Security: *Set Up: Security Fields* in the System functional area.

Context

Rule-based security enables you to create conditional rules to constrain members on a baseline security group. Workday supports specific report fields on business objects that you can use when defining rule conditions for a security rule. You can enable these report fields to make them available when creating a rule condition on the **Create Security Rule** task.

Steps

1. Access the **Maintain Fields for Security Rules** task.
2. Click **Add Fields for Security Rules**.
3. Select a business object from the **Business Object** prompt.
   You can only select 1 business object at a time.
4. Select the report fields that you want to enable on the **Fields** prompt.
5. Click **OK**.

Result

You can view a grid that displays all enabled fields and their business object.

Next Steps

Access the **Create Security Rules** task to create new security rules with the fields you enabled.

Related Information
Tasks
Create Security Rules on page 179

Example: Set Up Access Constraint Rules for Recruiters

This example illustrates how to create access constraint rules that restrict recruiters from accessing job requisitions in which they're both an applicant and recruiter.

Context

You want to prevent recruiters from applying for job requisitions they're recruiting for. You create a security rule with conditions that restrict users with the recruiter role from self-service access to applications. Finally, you create a rule-based security group that incorporates the security rule.

Prerequisites

Security: These domains in the System functional area:

- *Security Activation*

- *Security Configuration*
- *Set Up: Security Fields*
- *Set Up: Security Rules*

Steps

1. Access the **Maintain Fields for Security Rules** task.
   a) Select **Add Fields for Security Rules**.
   b) Specify these values:

Rule Usage Type	*Security Attribute - Context Instance*
Business Object	*Job Application*
Fields	*Worker*

   c) Click **OK**.
2. Access the **Create Security Rule** task.
   a) Specify these values:

Security Rule Type	*Access Constraint Rule*
Business Object	*Job Application*

   b) Click **OK**.
   c) Enter *Recruiter Access Constraint* in the **Description** field.
   d) Add a row to the **Rule Conditions** grid.
   e) Specify these values in the Rules grid:

And/Or	Security Field	Relational Operator	Comparison Type	Comparison Value
And	*Worker*	*In the selection list*	*Value from another field*	*Current Worker*

   f) Click **OK**.
3. Access the **Create Security Group** task.
   a) From the **Type of Tenanted Security Group** prompt, select *Rule-Based Security Group*.
   b) Enter Recruiter Job Applicants as the **Name**.
   c) Click **OK**.
   d) From the **Baseline Security Group** prompt, select the *Recruiter* role-based security group.
   e) Select *Use Membership from Baseline Security Group* in the **Membership** section.
   f) In the **Access to Instances** section, select *Exclude Access to Instances by Rule* and enter *Recruiter Access Constraint* in the prompt.
   g) Click **OK**.

Result

You can test the accuracy of your configurations using the **Test Security Rule** and **Test Security Group Membership** tasks.

Related Information
Tasks
Create Rule-Based Security Groups on page 178
Create Security Rules on page 179

Example: Set Up Rule-Based Security Groups

This example illustrates how to create a rule-based security group using a membership security rule.

Context

Currently, you enable all employees to enter their work time on Workday. You want to change your security configuration to ensure that only nonexempt U.S. employees can enter their work time on Workday.

Prerequisites

Security: These domains in the System functional area:

- *Security Activation*
- *Security Configuration*
- *Set Up: Security Fields*

Steps

Enable report fields for use in the security rules for the security group:

1. Access the **Maintain Fields for Security Rules** task.
2. Click **Add Fields for Security Rules**.

   You can only view the **Add Fields for Security Rules** button when you haven't enabled any fields yet. When a report field is already enabled, you'll view a grid that displays the business object and its enabled fields instead. For this case, click the **Edit** button on the business object to enable additional report fields.
3. Select *~worker~* from the **Business Object** prompt.
4. Select these fields from the **Fields** prompt:
   - *Location Address - Country*
   - *Exempt*
5. Click **OK**.

Create the security rule:

6. Access the **Create Security Rule** task.
7. Specify these values:

Option	Description
Security Rule Type	*Membership Rule*
Business Object	*Worker*

8. Click **OK**.
9. Enter *Exempt U.S. Security Rule* in the **Description** field.
10. Add a second row on the **Rule Conditions** grid.
11. Select these values on the **Rule Conditions** grid:

And/Or	Security Field	Relational Operator	Comparison Type	Comparison Value
And	*Location Address - Country*	*in the selection list*	*Value specified in this filter*	*United States of America*
And	*Exempt*	*equal to*	*Value specified in this filter*	Clear the check box.

12. Click **OK**.
13. Access the **Create Security Group** task.

14. Specify these values:

Option	Description
Type of Tenanted Security Group	*Rule-Based Security Group*
Name	*Non-Exempt U.S. Employees*

15. Click **OK**.
16. Select *Employee As Self* from the **Baseline Security Group** prompt.
17. Select *Include Members by Rule* in the **Membership** section.
18. Select **Exempt U.S. Security Rule** from the prompt.
19. Click **OK**.
20. Select **Domain** > **Edit Security Policy Permissions** from the related actions menu of the *Self-Service: Time Tracking High Volume* domain.
21. Replace *Employee As Self* with *Non-Exempt U.S. Employees* on the **Report/Task Permissions** grid.
22. Click **OK**.
23. Access the **Activate Pending Security Policy Changes** task.
24. Enter *Enabling only nonexempt U.S. employees to enter their work time* in the **Comment** field.
25. Click **OK**.
26. Click **Confirm**.
27. Click **OK**.

Result

Nonexempt U.S. employees can access the **Enter My Time** task. Non-U.S. employees and U.S. exempt employees are among the workers who can no longer access the task.

Related Information

Tasks

Create Rule-Based Security Groups on page 178

Create Security Rules on page 179

FAQ: Rule-Based Security Groups

- How many membership security rules can I select on a rule-based security group? on page 183
- Should I rerun the Activate Pending Security Policy Changes task when I change a security rule? on page 184
- Why can't I access certain report fields on the Worker business object when I configure a security rule? on page 184
- Why can’t I access the security rules that display on my rule-based security group? on page 184
- How do I migrate rule-based security groups and security rules between tenants? on page 184
- What time zone does Workday use to evaluate whether a user is a member of a rule-based security group? on page 184

How many membership security rules can I select on a rule-based security group?

You can select 1 membership security rule for each rule-based security group. You can also:

- Add or change the rule conditions on a security rule.
- Combine the rule conditions from other security rules.

To combine existing conditions, add security rules to the **Copy Condition from Rule** prompt on the **Create Security Rule** task.

Should I rerun the Activate Pending Security Policy Changes task when I change a security rule?

You don't need to rerun the task when you change a security rule.

Why can't I access certain report fields on the Worker business object when I configure a security rule?

Workday enables you to access a subset of the report fields on the Worker business object. Workday provides these report fields:

- **Active Status**
- **Cost Center**
- **Has Active Flexible Work Arrangement**
- **Hire Date**
- **Job Level - Primary Position**
- **Management Level - All Positions**
- **Organization Membership**
- **Organization Roles**
- **Pay Group**
- **Professional Affiliations Reference**
- **Schedulable Worker**

Workday currently provides the subset of report fields based on these prioritized use cases:

- Enable managers who have active contingent workers in their departments to share reports on contingent workers.
- Enable only nonexempt US employees to clock in and out.
- Enable only US employees to access benefits information.
- Provide access based on worker type or compensation grade.
- Provide restricted self-service access to temporary employees and employees on leave.

Why can’t I access the security rules that display on my rule-based security group?

You can access security rules on rule-based security groups only when you can access the:

- Report fields on the security rules.
- *Set Up: Security Rules* domain or *Security Administration* parent domain in the System functional area.

How do I migrate rule-based security groups and security rules between tenants?

Implementers can use web services to migrate security rules and rule-based security groups. The web service used to migrate rule-based security groups only migrates the rule-based security group, its baseline security group, and any associated security rules. The web service doesn't include data that supports the baseline security group.

What time zone does Workday use to evaluate whether a user is a member of a rule-based security group?

Workday uses the preferred time zone for a user to evaluate membership on rule-based security groups. When a user doesn't have a preferred time zone, Workday defaults to this order to determine the time zone to use:

1. The time zone on the location of the user's primary position.
2. The tenant default time zone.
3. The Pacific Standard Time (PST) time zone.

When a user changes their time zone, Workday uses the new time zone once the user signs out and then signs in.

Related Information
Tasks
Create Rule-Based Security Groups on page 178
Examples
Example: Set Up Rule-Based Security Groups on page 182

Segment-Based Security Groups

Create Segment-Based Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use segment-based security groups to enable members of other security groups to access select components of a securable item. Members can be part of multiple security groups and have permission to access multiple security segments. Workday enables you to define security segments when you belong to a security group with Modify permissions on the *Set Up: Security Segments* domain.

Steps

1. Access the **Create Security Group** task.
2. From the **Type of Tenanted Security Group** prompt, select **Segment-Based Security Group**.
3. Under **Group Criteria**, select **Security Groups** that you want to access securable items.
4. From the **Access to Segments** prompt, select security segments that you want members of the specified security groups to be able to access.

   You can't combine security segments of different types in a segment-based security group.
5. Add the security group to security policies.
6. Activate pending security policy changes.

Next Steps

Users with access to a domain through both a segment-based and a non-segment-based security group have permission to access all segments. Make sure you associate non-segment-based security groups with users who have permission to access all segments by:

- Reviewing all security groups on the policy before adding segment-based security groups.
- Reviewing the included security groups in an aggregation security group.

Related Information
Tasks
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Example: Create Segment-Based Security Groups to Access Benefits-Related Documents

This example illustrates 1 way to use segment-based security groups to grant access to benefits-related documents.

Context

You want a Benefits Administrator to manage benefits-related documents, but not payroll-related documents. Workday secures access to manage all worker documents to the *Worker Data: Add Worker Documents* and *Worker Data: Edit and Delete Worker Documents* domains. You create a *Document Categories - Benefits* segment to identify benefits-related documents. You then use the security segment to create a segment-based security group so Benefits Administrators can access only benefits-related documents. You can also use this approach to secure payroll or hiring-related documents.

Prerequisites

These domains in the System functional area:

- *Security Activation*
- *Security Configuration*
- *Set Up: Document Category Security Segments*

Steps

1. Access the **Create Document Category Security Segment** task.
   a) In the **Name** field, enter *Document Categories - Benefits*.
   b) Select *Benefits* from the **Document Category** prompt.
   c) Click **OK** and **Done**.

   Note: Workday also delivers document categories and other security segments. As you determine which categories to create or use in a security group, consider the trade-off that comes with more granular categories. The more categories that you create or use, the more flexibility and range of access you'll provide in configuring segment-based security groups. Greater granularity also requires more configuration maintenance by additional security groups.
2. Access the **Create Security Group** task.
   a) Select *Segment-Based Security Group* from the **Type of Tenanted Security Group** prompt.
   b) In the **Name** field, enter *Benefits Administrator*.
   c) Click **OK**.
   d) From the **Security Groups** prompt, select *Benefits Administrator*.
   e) From the **Security Segments** prompt, select *Document Categories - Benefits*.
   f) Click **OK** and **Done**.
3. Access the **Maintain Permissions for Security Group** task.
   a) For the **Operation** type, select **Maintain**.
   b) From the **Source Security Group** prompt, enter *Benefits Administrator*.
   c) Under **Domain Security Policy Permissions**, add rows for the *Worker Data: Add Worker Documents* and *Worker Data: Edit and Delete Worker Documents* domains, with **View and Modify** access.
   d) Click **OK** and **Done**.
4. Activate Pending Security Policy Changes.

Related Information

Reference

Reference: Security Group Types on page 133

Examples

Example: Set Up Expense Item Segment Access with Aggregation Security Groups on page 149

Service Center Security Groups

Create Service Center Security Groups

Prerequisites

- Create a Service Center and Service Center representatives.
- Security: *Security Configuration* domain in the System functional area.

Context

You can use service center security groups to grant third-party users access to Workday. You can create:

- Constrained service center security groups so third-party users can support select organizations.
- Unconstrained service center security groups so third-party users can support all organizations.

Steps

1. Access the **Create Security Group** task.
2. In the **Group Criteria** section, select the Service Centers that you authorize to provide services for organizations.
3. (Constrained only) As you complete the task, consider:

Option	Description
Applies to Current Organization Only	Service Center representatives in the specified Service Centers can access securable items for the select organizations.
Applies to Current Organization And All Subordinates	Service Center representatives in the specified Service Centers can access securable items for the select organizations and all subordinate organizations.

The organization type from the organization criteria must match the organization type from the security group restrictions. Example: When you select Company, you can add the security group to only security policies restricted to the Company organization type.

Example

You want to hire temporary workers to assist with the benefits enrollment process. Instead of hiring the workers through the typical staffing process, you can provide the workers with temporary access by creating a service center. You can use the service center to create a service center security group. You can then assign the security group to the same domains assigned to the Benefits Administrator security group. As a result, temporary workers can assist with the enrollment process without going through the typical staffing process.

Next Steps

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information
Tasks
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Examples

Example: Create a Service Center Security Group for Benefits Support on page 188

Example: Create a Service Center Security Group for Benefits Support

This example illustrates 1 way to create an aggregation security group that includes the service center security group for each supported location.

Context

Your organization hires third-party users to provide benefits support to workers in the U.S. and Canada. You want to create separate service centers to support workers in different locations, but you don't want to assign permissions to each service center individually. You can create an aggregation security group that includes the individual security groups so you can more easily assign permissions to the security groups.

Prerequisites

Create U.S. and Canada service centers for third-party auditors.

Security: *Security Configuration* domain in the System functional area.

Steps

1. Create a security group for the U.S. service center.
    a. Access the **Create Security Group** task.
    b. Select *Service Center Security Group (Constrained)* from the **Type of Tenanted Security Group** prompt.
    c. Enter *U.S. Benefits* in the **Name** field.
    d. Click **OK**.
    e. Select *United States* from the **Organizations** prompt.
    f. Select *Applies to Current Organization And All Subordinates*.
    g. Click **OK**.
2. Create a security group for the Canada service center.
    a. Access the **Create Security Group** task.
    b. Select *Service Center Security Group (Constrained)* from the **Type of Tenanted Security Group** prompt.
    c. Enter *Canada Benefits* in the **Name** field.
    d. Click **OK**.
    e. Select *Canada* from the **Organizations** prompt.
    f. Select *Applies to Current Organization And All Subordinates*.
    g. Click **OK**.
3. Create an aggregation security group for all service centers.
    a. Access the **Create Security Group** task.
    b. Select *Aggregation Security Group* from the **Type of Tenanted Security Group** prompt.
    c. Enter *All Benefits Support* in the **Name** field.
    d. Click **OK**.
    e. Select *U.S. Benefits* and *Canada Benefits* from the **Security Groups to Include** prompt.
    f. Click **OK**.

4. Set security access to some of the benefits-related secured items.
    a. Access the **Maintain Permissions for Security Group** task.
    b. Select *Maintain* from the **Operation** field.
    c. Select *All Benefits Support* from the **Source Security Group** prompt.
    d. Click **OK**.
    e. Add a row on the **Domain Security Policy Permissions** grid.
    f. Select *View Only* from the **View/Modify Access** prompt.
    g. Select these domains from the **Domain Security Policy** prompt:
        - *Job Information*
        - *Worker Data: Compensation*
        - *Worker Data: Job Details*
        - *Worker Data: Public Worker Reports*
        - *Worklet General*
    h. Continue to add security domains for all service center representatives.
    i. Click **OK**.
5. Activate pending security policy changes.
    a. Access the **Activate Pending Security Policy Changes** task.
    b. Enter *Enabling third-party users to access tasks and reports to support employee benefits in Workday* in the **Comment** field.
    c. Click **OK**.
    d. Select the **Confirm** check box.
    e. Click **OK**.

Result

You can assign permissions to service center representatives in all locations using the All Benefits security group.

Related Information

Tasks

Create Aggregation Security Groups on page 149
Create Service Center Security Groups on page 187
Maintain Security Group Permissions on page 129

User-Based Security Groups

Create User-Based Security Groups

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can use user-based security groups to:

- Give administrators enterprise-wide access to the tenant.
- Grant specific workers permission to access items secured to a security policy.
- Administer another user-based security group. Workday enables you to add more than 1 administering security group.

You can't:

- Add user-based security groups to intersection security groups.

- Restrict user-based security groups to regions.

Steps

1. Access the **Create Security Group** task.
2. (Optional) From the **Administered by Security Groups** prompt, select 1 or more user-based security groups. Members of the specified security groups can assign users to the new user-based security group.

   Administrators with permission to the *User-Based Security Group Administration* domain can assign users to any user-based security group.

Example

You want to enable certain employees to create and maintain all bank setup data regardless of their organization. You can create a Bank Administrator user-based security group by directly assigning users to the security group. You can then add the security group to the *View: Bank Entity* and *Set Up: Cash Forecasting* domains to enable the assigned users to administer bank setup data. As you hire new employees to administer bank setup data, you can assign the employees to the security group directly.

Next Steps

Add users to the user-based security group. To add a user to:

- 1 user-based security group, access the **Assign User to User-Based Security Group** task or the workflow-enabled **Update User-Based Security Group Assignments** task.
- More than 1 user-based security group, access the **Assign User-Based Security Groups for Person** task.

Workday recommends disabling both **Assign** user-based security group tasks before using the workflow-enabled **Update User-Based Security Group Assignments** task.

To disable both non-workflow-enabled tasks:

1. Disable the *User-Based Security Group Administration* domain security policy.
2. Activate pending security policy changes
3. Access the **Maintain Feature Opt-Ins** report and opt into the **Disable User-Based Security Group Assignment Tasks** feature.

After you add users to the security group:

- Add the security group to security policies.
- Activate pending security policy changes.
- Activate the security group when you want to enable the permissions on an inactive security group.

Related Information

Tasks

Steps: Change User-Based Security Group Assignments for a User on page 191
Edit Domain Security Policies on page 200
Edit Business Process Security Policies on page 201
Activate Pending Security Policy Changes on page 203

Examples

Example: Create a User-Based Security Group for Administrators on page 192

Steps: Change User-Based Security Group Assignments for a User

Prerequisites

Before using the workflow-enabled initiating action to change a user's user-based security groups, disable existing non-workflow-enabled tasks by accessing the **Maintain Feature Opt-Ins** report and opting into the **Disable User-Based Security Group Assignment Tasks** feature.

Context

Workday enables you to configure a workflow-enabled initiating action to change a user's user-based security group assignments. By defining a new business process and related definition, you can ensure that changes in membership to user-based security groups go through the appropriate review and approval steps. For this feature, Workday doesn't support the use of organization-based security groups to create business process definitions.

Steps

1. Enable the*Process: User-Based Security Group Event* domain security policy in the System functional area.

   Security: *Process: User-Based Security Group Event* domain in the System functional area.

   See Steps: Enable Functional Areas and Security Policies
2. Configure the *User-Based Security Event for User* business process security policy.

   As you configure this business process, you can specify which security groups can perform workflow-specific actions, including Approve, Ad Hoc Approval, Cancel, Deny, Request Reassignment, View All, and View Completed Only.

   See Edit Business Process Security Policies
3. Create the *User-Based Security Event for User* business process default definition.

   We recommend including at least 1 reviewer or approver for each event, including the initiation of the **Review User Based Security Groups to Persons** task, Review, and Approval. You can also enable **Advanced Routing Restrictions** if the security group is the same for initiation and other business process tasks.

   While you can route business process steps to unconstrained security groups, Workday also enables you to contextually route to constrained role-based security groups, including roles assigned to Company, Company Hierarchy, Supervisory, Cost Center, Cost Center Hierarchy, Custom, and Location Hierarchy. Example: You add a Review step to the business process definition, specifying the Manager role-based security group as the reviewer. When you initiate changes in a user's security group assignments, the business process should contextually route to that user's manager.

   See: Steps: Configure Business Process Definitions
4. From users' related actions menu, access the **Update User-Based Security Group Assignments** initiating action.

   You can add or remove user-based security groups from a user's current assignments. As you navigate the initiating action, include a comment to record the changes you make to a user's security groups.
5. Activate pending security policy changes.

Related Information
Reference
2024R1 What's New Post: User-Based Security Framework
Examples
Example: Maintain User-Based Security Group Assignments on page 194

Steps: Change Membership for a User-Based Security Group

Prerequisites

Before using the workflow-enabled task to change the users in a user-based security group, disable existing non-workflow-enabled tasks by accessing the **Maintain Feature Opt-Ins** report and opting into the **Disable User-Based Security Group Assignment Tasks** feature.

Context

Workday enables you to configure a workflow-enabled initiating action to modify a user-based security group's membership. By defining a new business process and related definition, you can ensure that membership updates to a security group go through the appropriate review and approval steps. For this feature, Workday doesn't support the use of organization-based security groups to create business process definitions.

Steps

1. Enable the Process: User-Based Security Group Event domain security policy in the System functional area.

   Security: *Process: User-Based Security Group Event* domain in the System functional area.

   See: Steps: Enable Functional Areas and Security Policies
2. Configure the *User-Based Security Group Event for Group* business process security policy.

   As you configure this business process, you can specify which security groups can perform workflow-specific actions, including Approve, Ad Hoc Approval, Cancel, Deny, Request Reassignment, View All, and View Completed Only.

   See: Edit Business Process Security Policies
3. Create the *User-Based Security Group Event for Group* business process default definition.

   We recommend including at least 1 reviewer or approver for each event, including the initiation of the **Review User Based Security Groups to Persons** task, Review, and Approval. You can also enable **Advanced Routing Restrictions** if the security group is the same for initiation and other business process tasks.

   Workday enables you to route Initiate, Approve, and Review business process steps to a User-Based Security Group Administrators security group. This security group is populated with members of the updated security group's **Administered by Security Groups** field. If the field is left blank, steps in the business process will go unassigned. Example: You add a Review step to the business process definition, specifying the User-Based Security Group Administrators security group as the reviewer. If the Security Administrator security group is in the **Administered by Security Groups** field and multiple users are members of that administrator group, the business process will route to those administrators for review.

   See: Steps: Configure Business Process Definitions
4. Access the **Update User-Based Security Group Membership** initiating action.

   You can add or remove users from a user-based security group. As you navigate the initiating action, include a comment to record the changes you make to a security group's members.
5. Activate pending security policy changes.

Related Information
Reference
Feature Release Note: User-Based Security Group Membership Workflow

Example: Create a User-Based Security Group for Administrators

This example illustrates 1 way to set security permissions for administrators using a user-based security group.

Context

You recently hired a new Compensation Administrator who needs unconstrained access to worker compensation data. You can create a user-based security group and assign the new Compensation Administrator to the security group. As you hire additional Compensation Administrators, you can assign them to the security group without needing to reassign the security permissions.

Steps

1. Create a Compensation Administrator user-based security group.
   a. Access the **Create Security Groups** task.
   b. Select *User-Based Security Group* from the **Type of Tenanted Security Group** prompt.
   c. Enter *Compensation Administrator* in the **Name** field.
   d. Click **OK**.
   e. Select *Security Administrator* from the **Administered by Security Groups** prompt.
   f. Click **OK**.
2. Assign users to the user-based security group.
   a. Access the **Assign Users to User-Based Security Group** task.
   b. Select *Compensation Administrator* from the **Assign Users to User-Based Security Group** prompt.
   c. Click **OK**.
   d. Select 1 or more users to provide compensation administrator privileges from the **System Users** prompt.
   e. Click **OK**.
3. Assign security permissions to the user-based security group.
   a. Access the **Maintain Permissions for Security Group** task.
   b. Select *Maintain* from the **Operation** field.
   c. Select *Compensation Administrator* from the **Source Security Group** prompt.
   d. Click **OK**.
   e. Add a row on the **Domain Security Policy Permissions** grid.
   f. Select *View and Modify* from the **View/Modify Access** prompt.
   g. Select these domains from the **Domain Security Policy** prompt:
      - *Compensation Change: Salary*
      - *Set Up: Compensation*
      - *Worker Data: Compensation*
      - *Worker Data: Compensation Management*
   h. Continue to add security domains for Compensation Administrators.
   i. Click **OK**.

   Note: Workday restricts administrators from initiating certain transactions for themselves, including compensation change requests.
4. Activate your pending security policy changes.
   a. Access the **Activate Pending Security Policy Changes** task.
   b. Enter *Enabling compensation administrators to set up compensation components* in the **Comment** field.
   c. Click **OK**.
   d. Click **Confirm**.
   e. Click **OK**.

Related Information

Tasks

Create User-Based Security Groups on page 189

Maintain Security Group Permissions on page 129

Example: Maintain User-Based Security Group Assignments

This example illustrates 1 way to initiate, modify, and review changes to a user's membership to user-based security groups.

Context

You want to review and modify another administrator's security group assignments, so that you can remove them from a group that provides too much access to sensitive payroll information. After setting up the workflow-enabled task, you want to:

- Initiate the task.
- Restrict a user's membership to payroll-specific user-based security groups.
- Route the request to other administrators in your organization to review and approve the assignment.
- Verify the change in assignment using security reporting in Workday.

Prerequisites

Security: *Process: User-Based Security Group Event* domain in the System functional area.

Steps

1. Set up the workflow-enabled **Update User-Based Security Group Assignments** task.
   a) Enable the *Process: User-Based Security Group Event* domain security policy.
   b) Configure the *User-Based Security Group Event* business process security policy.
   c) Create the *User-Based Security Group Event* business process default definition.

   See Steps: Assign Users to User-Based Security Groups
2. Remove the user from payroll-specific user-based security groups.
   a) From the user's related actions menu, select **Security Profile** > **Update User-Based Security Assignments**.
   b) Remove these user-based security groups from the user's assignments:
      - *Payroll Administrator*
      - *Payroll Approver*
      - *Payroll Calculations Administrator*
      - *Payroll Integration Administrator*
   c) In the **Comment** field, enter *Removing Payroll access for [this user]*.
   d) Click **OK** and **Done**.
3. As another administrator, receive the security group assignment **Review** request in **My Tasks**.
   a) Confirm that **Details to Review** contains accurate information, including the user, supervisory organization, and security groups to **Grant Access To** and **Revoke Access To**. For the **Review** step, administrators can modify the requested security groups that are in the **Grant Access To** and **Revoke Access To** categories.
   b) Click **Approve**. The request routes to another member of your organization for final approval.

   The final approver can't modify the security groups on the request.
4. Access the **Security History for User** report to confirm that a user's account reflects the approved changes.

Next Steps
Activate pending security policy changes.
Related Information
Tasks
Steps: Change User-Based Security Group Assignments for a User on page 191

Reference

2024R1 What's New Post: User-Based Security Framework

Security Policies

Setup Considerations: Security Policies

You can use this topic to help make decisions when planning your configuration and use of security policies. It explains:

- Why to set them up.
- How they fit into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What They Are

Security policies enable you to configure access to groups of items and individual business process actions. By associating security groups with security policies, you can enable members of the security groups to access the secured items and actions.

Workday delivers these types of security policies:

- Domain security policies, which secure reports, tasks, and integrations.
- Business process security policies, which secure business processes.

Workday enables you to configure permissions for reports and tasks separately from permissions for integrations. You can set:

- Get and Put permissions for integrations.
- View and Modify permissions for reports and tasks.

You can also set various permissions for actions on business processes, such as View All, Rescind, and Deny permissions. View All permissions enable you to see a business process event, regardless of status.

Business Benefits

Security policies enable you to deliver the right information and actions to the right users. By configuring:

- Domain security policies, you can efficiently set permissions for groups of items rather than for individual items.
- Business process security policies, you can decide who can take actions on a business process.

Use Cases

- Add security groups to the Initiate permission on the *Change Job* business process security policy to enable members of the security groups to initiate job changes.
- Add security groups to the *Report Prompt Set Management* domain security policy to enable members of the security groups to create report prompt sets.
- Remove security groups from the *Photo Change* business process security policy to prevent members of the security groups from changing their photos.

Questions to Consider

Questions	Considerations
Do you want to provide users with access to certain information in a business process?	When you enable users to access business processes, Workday doesn't automatically enable the users to access all the information they need access to in the business processes. Use the domains associated with the business processes to determine what the users can access in the business processes. Example: Managers who run the *Change Job* business process can't view job profile information until you add them to the *Staffing Actions: Job Profile* domain.
Do you want to provide users with access to certain actions on a business process?	Providing access to certain actions on a business process can also provide access to other actions on the business process. Example: Providing security groups with Correct permissions also provides the security groups with View All permissions for transactions that are cancelable. Review each business process security policy to understand the permissions that Workday inherently provides.
What security group types can you add to a domain security policy?	You can access the **Allowed Security Group Types** field on a domain to view the types of security groups you can add to a domain security policy. Make sure that the security group types you want to add match the security group types on the **Allowed Security Group Types** field.
Do you want to override permissions from a parent security policy?	Workday defines parent-child relationships among domains so child security policies inherit permissions from a parent security policy. These relationships can help you maintain and update permissions for many items at once. You can override inherited permissions when a child security policy needs different permissions. When you override permissions on a child security policy, the other child security policies still inherit permissions from the parent policy. To reduce security policy maintenance, limit the number of child security policies you override. Example: You want managers to have access to all employee contact information except employee phone numbers. You can override the permissions on the security policy for employee phone numbers. **Note:** Upon breaking inheritance of a child policy, a new snapshot is created that shows the addition of any security groups included at the time of

Questions	Considerations
	activating policy changes. The new snapshot treats all security groups as new additions to the policy, including groups defaulted in from the original parent and any security groups you add or remove from the newly disinherited child.
When do you need to activate changes to security policies?	Changes to security policies only go into effect when you activate the changes. You only need to activate pending changes when you change a security policy. You don't need to activate these types of changes: • Assign roles. • Assign users to security groups. • Change a security group. • Create a security group.
Do you want to undo activated changes to security policies?	Workday enables you to revert to previous timestamps, undoing changes to security policies that you've activated. When you activate a previous timestamp, Workday retains the security configuration from the original timestamp as pending changes. If you don't want to reactivate those pending changes, cancel the changes, and then run the **Activate Pending Security Policy Changes** task. Example: You revert to a timestamp from September so you can eliminate the changes from October. After you revert to the previous timestamp, cancel the pending changes and activate pending security policy changes.

Recommendations

Consider all the items that you're providing access to when you assign a security group to a domain security policy.

Find the domains that secure the content you're looking to secure using the **View Security for Securable Items** report.

Requirements

Workday groups functionally similar domains and business processes into functional areas. To set permissions for domains and business processes, enable each functional area as well as its security policies. Enabling a functional area doesn't automatically enable all the security policies within the functional area.

When you remove a security group from a business process security policy, also remove it from the steps in the business process definition that reference the security group. Otherwise, Workday might not assign the steps in the business process to users, causing the business process to stall and requiring you to intervene.

Limitations

You can't:

- Change the actions available on business process security policies.
- Change the items within domains.
- Configure security policies to enable administrators to initiate transactions for themselves, such as requesting compensation changes.
- Create your own functional areas.
- Delete security policies.
- Move domains or business processes from 1 functional area to another.

Tenant Setup

No impact.

Security

These domains in the System functional area:

Domains	Considerations
Security Administration	Enables you to access security administration tasks and reports. Includes tasks for activating changes to security policies and reports for security audits.
Security Configuration	Enables you to access security configuration tasks and reports. Includes reports for analyzing and reviewing the configuration of security policies.

Business Processes

No impact.

Reporting

These reports enable you to audit security policies for business processes:

Reports	Considerations
Business Process Security Policies Changed within Time Range	Displays the changes to a business process security policy, who made the change, and when they made the change within a time frame. If you made multiple changes to a business process security policy within a time frame, only the latest change will return in the report.
Business Process Security Policies for Functional Area	Displays the security configuration for each business process security policy in a functional area.
Business Process Security Policies with Pending Changes	Displays each business process security policy with a pending change, who made the change, and when they made the change.
Business Process Security Policy History	Displays the changes to a business process security policy, who made the change, and when they made the change.

These reports enable you to audit security policies for domains:

Reports	Considerations
Domain Security Policies Changed within Time Range	Displays the changes to a domain security policy, who made the changes, and when they made the changes.
Domain Security Policies for Functional Area	Displays the security configuration for each domain security policy in a functional area.
Domain Security Policies with Pending Changes	Displays each domain security policy with a pending change, who made the change, and when they made the change.
Domain Security Policy History	Displays the changes to a domain security policy, who made the change, and when they made the change.
Domain Security Policy Summary	Displays the current security configuration for each domain.
Secured Items in Multiple Domains	Displays every secured item that Workday secures to more than 1 domain.

These reports provide more general support for security policies and functional areas:

Reports	Considerations
Audit Trail - Security	Displays the changes to security policies and permissions within a time frame.
Functional Areas	Displays all functional areas and the domains and business processes within them.
View All Security Timestamps	Displays all security timestamps and identifies the current active timestamp.
View Security for Securable Item	Displays how Workday secures delivered items, such as reports, tasks, integrations, business processes, and data sources.

Integrations

Integrations and other applications that access Workday must have an Integration System User (ISU) with:

- Get and Put access to the domains that secure web service operations.
- View access to the domains that secure report data sources and report fields.

Outbound EIBs also require access to the custom report used as a data source.

Workday secures each REST method to a domain or business process security policy. Each REST method can access only the domains and business processes that the current user can access. Example: The GET /supervisoryOrganizations REST API returns only the organizations that the user has permission to access.

Connections and Touchpoints

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Other Impacts

In addition to using segmented security, you can limit access to items in a domain through View permissions. When you set View permissions, members of the associated security groups can access only the items that users can view. Example: A domain includes 6 reports and 4 tasks. By setting View permissions, members of the associated security groups can only access the 6 reports.

You can use the **Maintain Permissions for Security Group** task to add 1 security group to many security policies at once.

Related Information

Concepts

Setup Considerations: Security Groups on page 122

Concept: Business Processes

Concept: Configurable Security on page 112

Concept: Security Policies on page 201

Concept: Security Policy Change Control on page 204

Tasks

Steps: Enable Functional Areas and Security Policies on page 111

Edit Domain Security Policies

Prerequisites

Security: *Security Configuration* domain in the System functional area.

As you configure rule-based security groups, security rules, and access constraint rules, consult the **Allowed Rule-Based Security Group Types** field on domains to verify that your configurations are enabled for and match those of a domain.

Context

Domain security policies secure access to items, like tasks, reports, integrations, or worklets. By editing a security policy, you can configure the level of access security groups have to those items.

Steps

1. Access the **Domain Security Policies for Functional Area** report.
2. Select a security policy.
3. Click **Edit Permissions**.
4. (Optional) Add a row to the grid.
5. Select groups from the **Security Groups** prompt.
6. Check the **View** or **Modify** box to grant security groups access to the report or task securable items.
7. Check the **Get** or **Put** box to grant security groups access to integration and report or task securable actions.
8. Click **OK**.
9. Activate pending security policy changes.

Result

Depending on the edits made to a domain security policy, users will have **View**, **Modify**, **Get**, or **Put** access. You can also modify users' access rights by changing their security group membership. Group membership is based on a person's role, organization, or other mechanisms.

Example
You want to provide HR Partners view-only access to the *Pre-Hire Data: Background Check Status* domain security policy. After accessing the **Domain Security Policies for Functional Area** report, select **Pre-Hire Process** > **Pre-Hire Data: Background Check Status** > **Edit Permissions**. Once you add a new row to the **Report/Task Permissions** table, enter the HR Partner security group and check **View**. Activate pending security policy changes.

Related Information

Concepts

Concept: Security Policies on page 201

Tasks

Activate Pending Security Policy Changes on page 203

Edit Business Process Security Policies

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can specify which security groups have permission to access each of the securable items in a business process security policy.

Hierarchical relationships in business process security policies logically group similar policies, but there's no inheritance.

Steps

1. Access the **Edit Business Process Security Policy** task.
2. Select a **Business Process Type** from the prompt.
3. Add or remove security groups for each relevant action on the business process.
4. If you removed a security group from a business process security policy, remove that group from the corresponding business process definition.

   See: Edit Business Processes.
5. If you want to compare the existing business process security policy to the policy with pending changes implemented, access **View Pending Changes** from the related actions menu of the security policy.
6. Activate Pending Security Policy Changes on page 203.
7. Access the **Start Proxy** task to confirm that members of security groups with edited permissions have the appropriate level of access.

Next Steps

If you want to revert security policy changes, you can run the **Activate Previous Security Timestamp** task.

Related Information

Tasks

Activate Pending Security Policy Changes on page 203

Edit Business Processes

Edit Domain Security Policies on page 200

Concept: Security Policies

A security policy secures the items in a domain or business process. Each functional area can contain security policies for:

- Actions, such as action steps, approvals, and initiation steps on business processes.
- Reporting and task items, such as data sources, delivered worklets, report fields, reports, and tasks.
- Integration items, such as integration templates and web services.

For each functional area, you can view the security policies for:

- Domains by accessing the **Domain Security Policies for Functional Area** report.
- Business processes by accessing the **Business Process Security Policies for Functional Area** report.

By selecting **Edit Permissions** on a security policy, you can assign or remove security groups from the security policy to modify permissions to secured items. However, you can't:

- Change the securable items in a security policy.
- Define more than 1 security policy for a domain or business process.
- Delete a security policy.
- Move a domain or business process from 1 functional area to another.

When you configure the security policy for a business process, Workday:

- Displays an Initiation step for each way to start the business process.
- Enables you to specify whether you can delegate the business process to others.
- Includes separate securable items for each Action step in the business process.

For each update, Workday creates empty domain security policies that you can configure. You can use the **Create Security Policy for Domain** task to create the security policy for a domain between updates. As you complete the task, the **For Domain** prompt displays only domains that don't already have associated security policies in your tenant.

Security Policy Assignments

You can assign users to security policies by:

- Assigning users to security groups.
- Deriving security group membership.

You can assign:

- Users to Workday-delivered or custom user-based security groups.
- Integration system users to integration system security groups.

You can derive security group membership based on relevant information about users. Examples: You can assign:

- The appropriate job profile during the hire or job change process.
- Users to the appropriate locations when you configure location-based security groups.
- Users to the appropriate organizations when you configure organization-based security groups.
- Worker positions to organization roles. When you need organization-specific security access, you can create organization roles and role-based security groups.

After you assign users to security groups or derive security group membership, assign the security groups to security policies using these tasks:

- **Edit Domain Security Policies**
- **Edit Business Process Security Policies**

Business Process Security Policies and Event Targets

An event is a business process transaction that occurs within your organization, such as hiring an employee. An event target is the instance that a business process event is about. Examples:

- For a *Hire* business process event, the event target is the person you're hiring.

- For an *Expense* business process event, the event target is the person responsible for the expense report.

To access an event target, you must have permission to access both the:

- Business process. Examples: *Hire*, *Expense Report Event*.
- Specific instances. Examples: Pre-hire, Employee.

When you lose access to an event target, you also lose access to an event involving the target. That is, unless you are in a security group with access to the event.

To hide comments and details of a business process event from only the person an event is for, use these check boxes on the business process security policy:

- **Hide Comments from Person**
- **Hide Details from Person**

The **Hide Details from Person** check box overrides the **Hide Comments from Person** check box. Meaning, if you only select the **Hide Details from Person** check box, Workday hides both comments and details of the event.

Related Information
Concepts
Concept: Configurable Security on page 112
Concept: Security Groups on page 129
Reference
Reference: Security-Related Reports on page 114

Security Change Control

Activate Pending Security Policy Changes

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

Create an active timestamp using the **Activate Pending Security Policy Changes** task. Security policy changes made since the previous active timestamp take effect immediately. The active timestamp now reflects the current time, whether or not changes are pending.

You can run these reports to view a detailed list of the security policy changes you're activating:

- **Domain Security Policies with Pending Changes**
- **Business Process Security Policies with Pending Changes**

Steps

1. Access the **Activate Pending Security Policy Changes** task.
2. Describe your changes in the **Comment** field.
3. Select the **Confirm** check box to activate your changes.

Next Steps

You can use the **View All Security Timestamps** report to roll back to a previous timestamp.

Activate Previous Security Timestamp

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

Workday enables you to revert to a previous security timestamp for troubleshooting purposes. When you activate a previous timestamp, Workday prevents you from using the current timestamp again.

If you're recovering from a faulty configuration, activating a previous timestamp doesn't fix errors; it only evaluates your security configuration at an earlier point in time. The errors still exist and you must correct them before you run the **Activate Pending Security Policy Changes** task to create a new timestamp.

When you activate a previous timestamp, check for changes not governed by the security policy but that affect it. Example: A security group isn't part of the security policy that references it. You can delete a security group and change security policies to no longer reference that security group. However, the security group doesn't display if you activate a previous security timestamp referencing that security group. Changes made to a business process could mean that it’s no longer secured or routed correctly when you revert to a previous timestamp.

When you change the name of a security group, run the **Activate Pending Security Policy Changes** task to update security policies with the new name.

Steps

1. Access the **Activate Previous Security Timestamp** task.
2. From the **Previous Security Timestamps** prompt, select a previous timestamp.
3. (Optional) Describe your changes in the **Comment** field.
4. Select the **Confirm** check box. Workday timestamps the current moment, which includes these changes.

Result

Any security policy changes made after this timestamp are no longer in effect, but Workday preserves the changes as pending changes. Use the **Activate Pending Security Policy Changes** task to implement these changes.

Next Steps

You can edit your comments at any time. To edit your comments, select **Security Timestamp** > **Edit** from the related actions menu of the **View All Security Timestamps** report.

Related Information
Tasks
Activate Pending Security Policy Changes on page 203

Concept: Security Policy Change Control

Security policy change control enables you to:

- Revert to previous versions of your security configuration so you can correct critical security errors.
- Prepare complex security changes and activate the changes when you're ready to deploy them.

Security policy change control doesn’t enable you to retain alternate valid security configurations. When you revert from a security configuration, the security configuration is no longer available.

How It Works

With security policy change control:

- Workday records the time of every security change.
- Workday evaluates security as of a timestamp, ignoring pending changes until you activate your current security configuration.
- You can activate a previous timestamp.

Security timestamps take into account these changes:

- Adding or removing security groups from security policies.
- Enabling or disabling the delegation of business processes.
- Enabling or disabling security domains or functional areas.

These changes take effect immediately and don't require activation:

- Security group definitions.
- User assignments.

Example

You activate security policy changes in March, June, and September. In September, you discover a serious error in the security configuration from March. You decide to activate the timestamp from March by running the **Activate Previous Security Timestamp** task.

After you activate the timestamp, the June and September changes are pending. The changes you make to fix the error from September are also pending. When you run the **Activate Pending Security Policy Changes** task:

- Workday creates a new timestamp and activates all changes made since March.
- You can no longer activate the timestamp from September because Workday considers it an invalid configuration.

Exporting Security Changes

When you export security changes to a test tenant for validation, you can activate all changes at once.

Reporting

You can view an activated security policy and the pending changes by accessing:

- **Domain Security Policy** > **View Latest Version** from the related actions menu of a domain security policy.
- **Business Process Policy** > **View Latest Version** from the related actions menu of a business process security policy.

You can compare security policy versions, before and after changes, by accessing:

- **Domain Security Policy** > **View Pending Changes** from the related actions menu of a domain security policy.
- **Business Process Policy** > **View Pending Changes** from the related actions menu of a business process security policy.

Related Information
Reference
Reference: Security-Related Reports on page 114

Service Centers

Steps: Set Up Service Centers

Context

You can configure service centers to grant third-party organizations access to your Workday tenant, without granting them access to sensitive data. Service centers consist of representatives who work only for that service center and aren't part of your headcount.

That level of flexibility enables you to authorize service center representatives to access only certain information in your Workday tenant. If you want representatives to support only a subset of workers in your organization, you can assign them to a constrained security group. If you want a service center representative to have administrative-level access to your tenant, you can assign them to an unconstrained service center security group.

Steps

1. Access the **Create Service Center** task.

   (Optional) Enter contact information for the service center, not for individual representatives.

   Security: *Set Up: Service Center* domain in the System functional area.
2. Access the **Create Service Center Representative** task.

   (Optional) Enter contact information for new representatives, not for the service center.

   Security: *Manage: Service Center* domain in the System functional area.
3. (Optional) Create a business process definition for the service center using the *Create Workday Account* business process.

   See Create Workday Accounts for Service Center Representatives on page 207.
4. From the related actions menu of a representative, select **Security Profile** > **Create Workday Account**.

   Create a Workday account to enable the representative to sign in to your Workday tenant.
5. Set security permissions for the service center.

   See Assign Roles to Service Centers on page 207.
6. Set security permissions for representatives in the service center.

   See Create Service Center Security Groups on page 187.

Result

Service center representatives can perform tasks in your Workday tenant on specified items.

Example

Global Modern Services outsources its IT support to Global Technologies. Kevin, an employee of Global Modern Services, locks himself out of his account. You can configure a service center so a representative from Global Technologies can unlock his account.

Next Steps

Run the **View Service Center** report to view information about the service center and the service center representatives, including:

- Activation or inactivation dates.
- Changes in service center assignments.
- Contact information.

Related Information
Examples
Example: Create a Service Center for Third-Party Auditors on page 209

Assign Roles to Service Centers

Prerequisites

Configure the *Assign Roles* business process and security policy in the Organizations and Roles functional area.

Context

When you assign the Service Center Manager role to a Service Center, Service Center Managers can authorize representatives to perform tasks and access other secured items.

Steps

1. From the related actions menu of a service center, select **Roles** > **Assign Roles**.
2. Select a role from the **Assign Roles** grid.

   Make sure you can assign the role to users. You must be in a security group in the **Assigned/ Reviewed by Security Groups** field on the **Maintain Assignable Roles** task.

   Workday indicates whether you can assign a role to multiple users on the **Restricted to Single Assignment** field. You can modify the field on the **Maintain Assignable Roles** task.
3. Assign the role to one or more users.

Related Information
Tasks
Set Up Assignable Roles
Create Role-Based Security Groups on page 174
Create Service Center Security Groups on page 187

Create Workday Accounts for Service Center Representatives

Prerequisites

Create role-based security groups for Service Center Managers and add them to the *Manage: Service Center* security domain with View and Modify permissions.

Context

You can create different business process definitions for the *Create Workday Account* business process for each Service Center, enabling Service Center Managers to:

- Create or change a Workday account and notify the Security Administrator.
- Send email messages to the email address specified in their contact information.

Steps

1. View the definition of the *Create Workday Account (Default Definition)* business process.
2. From the related actions menu of the business process definition, select **Business Process** > **Copy or Link Business Process Definition**.
3. Select **Copy Workflow Definition to Business Object**.
4. From the prompt, specify the Service Center.

5. From the related actions menu of the business process definition for the Service Center, select **Business Process** > **Add Notification**.
6. Create notifications for the appropriate security groups, such as:
   - Security Administrator.
   - Service Center Representative as Self.

Result

Workday notifies members of the selected security groups when you create a Workday account for a Service Center representative.

Related Information

Tasks

Assign Roles to Service Centers on page 207
Create Custom Notifications
Edit Business Processes
Edit Workday Accounts on page 246

Manage Passwords for Workday Accounts

Prerequisites

Configure Service Center and Service Center representatives.

Security: These domains in the System functional area:

- *Workday Account Passwords*
- *Workday Accounts*

Context

Service Center representatives can reset and change passwords for workers in your Workday tenant. These steps only apply to Workday accounts, which are accounts that Workday manages.

Steps

1. From the related actions menu of a worker profile, select **Security Profile** > **Manage Workday Account Credentials**.
2. As you complete the task, consider:

Option	Description
Generate Random Password	Workday emails the worker a randomly generated password. When the worker signs in with the randomly generated password, Workday prompts them to create a new password.
New Password **Verify New Password**	Service Center representatives can configure a new password for the worker.
Require New Password at Next Sign In	Workday ignores this setting when users sign in using Delegated Authentication or SAML.
Reset Challenge Questions (Do Not Use)	Enables users who specified challenge questions to reset their challenge questions. When users don't specify challenge questions, you can't successfully clear the check box; Workday doesn't save changes to the check box.

Option	Description
	Note: Workday plans to retire challenge questions in a future release.

Related Information
Tasks
Configure Password Reset on page 253
Edit Workday Accounts on page 246

Inactivate Service Center Representatives

Prerequisites

Configure the *Inactivate Service Center Representative* business process in the System functional area.

Security: These domains in the System functional area:

- *Manage: Service Center*
- *Self-Service: Service Center Representative*

Context

As a Service Center Administrator, you can inactivate any Service Center representative. When you inactivate a Service Center representative, Workday:

- Disables their Workday account.
- Dissociates them from Service Centers.
- Removes their associated roles.

Workday also removes the representative from:

- All role-based security groups associated with the Service Centers.
- All Service Center security groups.
- Delegation.

Only users with unconstrained and Modify permissions can activate or inactivate a service center representative.

Steps

1. Access the **View Service Center Representative** report.
2. From the related actions menu of the Service Center representative, select **Service Center Representative** > **Inactivate**.
3. Select the **Confirm** check box.

Example: Create a Service Center for Third-Party Auditors

This example illustrates how to provide third-party auditors with read-only access to securable items using service centers.

Context

Your organization decides to engage temporary third-party auditors to complete audits of your tenant. Because the auditors are temporary engagements, you don’t want to onboard them through the typical staffing process. You only want to provide the auditors with temporary read-only access to reports for auditing. You can create a service center for the auditors to provide them with the right permissions quickly.

Prerequisites

Security: These domains in the System functional area:

- *Manage: Service Center*
- *Set Up: Service Center*

Steps

1. Create a service center to group together all third-party auditors.
   a. Access the **Create Service Center** task.
   b. Enter *Third-Party Auditors* in the **Name** field.
   c. Click **OK**.
2. Add each third-party auditor as a representative to the service center.
   a. Access the **Create Service Center Representative** task.
   b. Select *Third-Party Auditors* from the **Service Center** prompt.
   c. Enter *James* in the **First Name** field.
   d. Enter *Morgan* in the **Last Name** field.
   e. Click **OK**.
3. Create a Workday account for each auditor so they can sign in to your Workday tenant.
   a. From the related actions menu of the representative, select **Security Profile** > **Create Workday Account**.
   b. Enter *James.Morgan* in the **User Name** field.
   c. Enter a password for the new representative.
   d. Clear the **Require New Password at Next Sign In** check box.
   e. Click **Submit**.
4. Associate the representative with the System Auditor user-based security group. Workday associates the delivered security group with all the necessary items for auditing.
   a. Access the **View Security Group** report.
   b. Select *System Auditor* from the **Security Group** prompt.
   c. Click **OK**.
   d. From the related actions menu of the System Auditor security group, select **User-Based Security Group** > **Assign Users**.
   e. Specify *James Morgan* in the **System Users** field.
   f. Click **OK**.

   Note: If you want to provide auditors access to 1 company's data, you can create a service center security group and set the organization type to Company.

Result

Workday associates the domain that secures the items for auditing with the System Auditor security group. You can grant access to the items by assigning representatives to the security group.

Related Information

Tasks

Steps: Set Up Service Centers on page 206
Create Service Center Security Groups on page 187

Examples

Example: Create a Service Center Security Group for Benefits Support on page 188

Constrained Proxy

Steps: Set Up Constrained Proxy Access

Context

Workday enables you to configure constrained proxy access so that users can delegate tasks and reports to other users in any Workday environment. This eliminates the need to share passwords, enables you to audit user actions, and helps you comply with security best practices.

Steps

1. Set Up the My Proxy Worklet on page 212.
2. Set Up the Security Policy for the Proxy Approval Process on page 212.
3. Set Up the Proxy Approval Process on page 213.
4. Create Proxy Access Restriction Sets on page 214.
5. (Optional) Select **Business Process > Maintain Help Text** from the related actions menu of the *Constrained User Proxy* business process.

   Select a step and enter help text. Select a condition rule when you need to give different help text to different audiences.

   Security: *Business Process Administration* domain in the System functional area.

Result

Users can request proxy access on behalf of a worker using the **Request Proxy Access** task. Workday notifies the worker so the worker can approve or deny the request.

Users with proxy access can:

- Start proxy sessions using the **Start User Proxy** task.
- Stop proxy sessions using the **Stop User Proxy** task.

During proxy sessions, Workday displays **On Behalf of** and the name of the user on whose behalf a proxy user acts.

Example

As chief financial officer (CFO), Teresa wants to include important financial metrics in an upcoming presentation. Teresa delegates certain reports to Olivia, an executive assistant, so Olivia can export the financial metrics for the presentation. Teresa enables Olivia to access only the relevant reports that she needs in order to export the financial metrics.

Related Information

Concepts

Concept: Constrained Proxy on page 215

Reference

2021R1 What's New Post: Constrained Proxy

The Next Level: Introducing Constrained Proxy

Examples

Example: Set Up Constrained Proxy Access on page 216

Set Up the My Proxy Worklet

Prerequisites

Security: *Set Up: Tenant Setup - Worklets* domain in the System functional area.

Context

You can configure the **My Proxy Dashboard** worklet to display on the Home page for any Workday user. The worklet enables users to access their delegated tasks and reports quickly, making it easier for them to:

- Manage their proxy policies.
- Request proxy access on behalf of other users.
- Start and stop proxy sessions.

You can also access tasks and reports for configuring constrained proxy.

Steps

1. Access the **Maintain Dashboards** report.
2. Edit the **Home** dashboard.
3. Add a row for the worklet.
4. Select *My Proxy Dashboard* from the **Worklet** prompt.
5. Select security groups from the **Required for Groups** prompt if Workday doesn't autofill them.
   Workday recommends that you select the *Constrained User Proxy* security group.
6. Select the **Required?** check box to display the worklet on the Home page.

Related Information
Concepts
Concept: Constrained Proxy on page 215

Set Up the Security Policy for the Proxy Approval Process

Prerequisites

- Set up the **My Proxy Dashboard** worklet.
- Security: *Security Configuration* domain in the System functional area.

Context

You can configure the *Constrained User Proxy* business process to route proxy requests for approval. This business process enables you to specify who can:

- Approve or deny proxy access requests.
- Request proxy access.
- View notifications about policy changes.

Only security groups based on employee or contingent workers can approve proxy requests. Workday delivers these worker-based security groups:

- *All Employees*
- *All Contingent Workers*

Note: The first time you configure the *Constrained User Proxy* business process security policy, you can't add the *All Employees* and *All Contingent Workers* security groups to the **Who Can Start the Business Process** section. Complete the initial business process security policy set up, and then edit the policy again to select the *All Employees* and *All Contingent Workers* security groups.

Security groups not based on employee or contingent workers can't approve proxy requests. Examples of ineligible Workday-delivered security groups include:

- *All Pre-Contingent Workers*
- *All Pre-Employees*
- *All Service Center Representatives*

Steps

1. Access the **My Proxy Dashboard** worklet.
2. Select the **Edit Business Process Security Policy** task.
3. Select *Constrained User Proxy* from the **Business Process Type** prompt.
4. From the **Security Group** prompt in the **Who Can Start the Business Process** section, do 1 of these procedures:
   - Select a security group other than *All Employees* or *All Contingent Workers* and click **OK** to complete the task. Access the **Edit Business Process Security Policy** task again to select the *All Employees* and *All Contingent Workers* security groups.
   - Select *Create* and create a security group based on workers. Only employees or contingent workers can start the business process to approve proxy requests.
5. In the **Who Can Do Actions on Entire Business Process** section, add these security groups to the **View** action:
   - *Initiator*
   - *Employee As Self*
   - *Contingent Worker*

   Members of the security groups can access the **View Event** button on proxy access notifications and view their archived approvals.
6. In the **Who Can Do Actions on Entire Business Process** section, add these security groups to the **Approve** and **Deny** actions:
   - *Employee As Self*
   - *Contingent Worker As Self*

   Employees and contingent workers can approve or deny requests to access items on their behalf when you add the security groups.
7. Activate Pending Security Policy Changes on page 203.

Next Steps

Set up the proxy approval process.

Set Up the Proxy Approval Process

Prerequisites

- Set up the **My Proxy Dashboard** worklet.
- Set up the security policy for the proxy approval process.
- Security: These domains in the System functional area:
  - *Business Process Administration*
  - *Manage: Business Process Definitions*

Context

You can configure the *Constrained User Proxy* business process so users must approve requests to access securable items on their behalf. You only need to configure the proxy approval process once.

Steps

1. Access the **My Proxy Dashboard** worklet.
2. Select the **Create Business Process Definition (Default Definition)** task.
3. Select *Constrained User Proxy* from the **Business Process Type** prompt.
4. Add an *Approval* step to the business process definition:

Option	Description
Order	Enter the letter *b*.
Type	Select *Approval*.
Group	Select *Employee As Self* and *Contingent Worker As Self*.
Due Date	(Optional) Specify by when users must approve a request.

Result

Employees and contingent workers can request proxy access using the **Request Proxy Access** task. The *Constrained User Proxy* business process initiates when employees and contingent workers complete the task.

Next Steps

Create proxy access restriction sets.

Create Proxy Access Restriction Sets

Prerequisites

- Set up the **My Proxy Dashboard** worklet.
- Security: *Security Configuration* domain in the System functional area.

Context

Restriction sets are custom collections of tasks and reports. Users can request access to restriction sets so they can access tasks and reports on behalf of other users. Once users request access to restriction sets, you can't delete the restriction sets.

Steps

1. Access the **My Proxy Dashboard** worklet.
2. Select the **Maintain Proxy Access Restriction Sets** task.

3. Select tasks and reports to add to a restriction set from the **Secured Item** prompt. When Workday displays more than 1 securable item with the same name, you can refer to the:
   - Type of the securable item in parentheses.
   - Path to access the securable item in brackets.

   You can't add integrations and web services to restriction sets.

   If you add a composite report to a restriction set, you must also add its subreports.

   Workday displays a warning when you select a self-service securable item.

   Note: Workday prevents the addition of items secured by specific domains to restriction sets. These domains include:

   - Core Actions.
   - Core Navigation.
   - Internal Requests (public).
   - Manage: Payment Election.

Next Steps
Once you create a restriction set, users can complete the **Request Proxy Access** task to access the securable items specified in that restriction set.

Concept: Constrained Proxy

You can configure constrained proxy access so Workday users can delegate tasks and reports to other users in any Workday environment. Constrained proxy access exclusively enables proxy users to:

- Access only specified securable items for a specified duration.
- Perform delegated tasks on behalf of other users.
- Request access to items. You don't need to define rules for who can start proxy sessions.

Constrained proxy access also enables you to configure proxy access for any Workday environment.

Delegation

Constrained proxy and delegation enable users to share responsibility for secured items without permanently reassigning the items. The types of items you can delegate differ among constrained proxy and delegation. With:

- Constrained proxy, you can share responsibility for tasks and reports.
- Delegation, you can share responsibility for initiating tasks and other tasks from My Tasks associated with 1 or more business processes.

Excluded Functionality

Proxy users can't:

- Access business processes or business process attachments during proxy sessions.
- Access items from prompts secured to reports that aren't in approved restriction sets.
- Access features involving multiple tasks, including dashboards, hubs, and worklets.
- Download custom reports by printing the reports during proxy sessions.
- Start proxy sessions or perform actions as a delegate once they're in a constrained proxy session.
- Start proxy sessions using Workday on Android, iPad, or iPhone.

Workday doesn't support business process delegation for the *Constrained User Proxy* business process.

Auditing Proxy Access

You can run the:

- **All Constrained User Proxy Requests** report (secured to the Security Configuration domain) to view all approved constrained proxy requests for any user. The report is available from the **My Proxy Dashboard** worklet.
- **View User Activity** report to view the actions users perform in proxy sessions.

Users can run the **Manage My Constrained Proxy** report from the **My Proxy Dashboard** to:

- View and revoke access by others to items on their behalf.
- View the items that users can access on behalf of others.

You can configure the *Revoke Constrained Proxy Policies* service on a *Termination* business process definition to revoke proxy access for a terminated worker automatically.

Workday prevents a proxy user from performing actions in a proxy session when the user that they're acting on behalf of revokes their proxy access.

Updating Proxy Access Restriction Sets

Proxy users don't need to restart proxy sessions when you make changes to restriction sets.

Proxy users and the users they're acting on behalf of receive a notification when someone modifies a restriction set that's in use.

Migrating Proxy Access Restriction Sets

Implementers can use Workday-delivered web services to migrate restriction sets.

Related Information
Tasks
Steps: Set Up Constrained Proxy Access on page 211
Reference
Setup Considerations: Delegation
Next Level: Introducing Constrained Proxy

Example: Set Up Constrained Proxy Access

This example illustrates how to enable users to delegate securable items to other users by providing them with constrained proxy access.

Context

The chief financial officer (CFO) of your organization wants to review organization performance against budget in each revenue category. The CFO decides to delegate the relevant report to an assistant for 1 week so the assistant can generate the results. After that time, the CFO wants Workday to remove their access to the item.

Prerequisites

Security: These domains in the System functional area:

- *Business Process Administration*
- *Manage: Business Process Definitions*
- *Security Configuration*

Steps

1. Configure the My Proxy Dashboard worklet to display on the Home page.
   a. Access the **Maintain Dashboards** report.
   b. Edit the **Home** dashboard.
   c. Add a row for the worklet.
   d. Select *My Proxy Dashboard* from the **Worklet** prompt.
   e. Select *Constrained Proxy Users* from the **Required for Groups** prompt.
   f. Select the **Required?** check box to display the worklet on the Home page in proxy sessions.
   g. Click **OK**.
2. Create a restriction set.
   a. Select the **My Proxy Dashboard** worklet on the Home page.
   b. Access the **Maintain Proxy Access Restriction Sets** task.
   c. Enter *Report for Budget and Actual by Revenue Category* in the **Name** field.
   d. Enter *Generate results for organization performance compared to budget in each revenue category* in the **Description** field.
   e. Select the **Budget vs. Actual by Revenue Category** report from the **Securable Item** prompt.
   f. Click **OK**.
3. Specify who can approve or deny proxy access requests.
   a. Select the **My Proxy Dashboard** worklet on the Home page.
   b. Access the **Edit Business Process Security Policy** task.
   c. Select *Constrained User Proxy* from the **Business Process Type** prompt.
   d. Click **OK**.
   e. Select *Initiator*, *Employee As Self*, and *Contingent Worker As Self* for the View All action in the **Who Can Do Actions on Entire Business Process** section.
   f. Select *Employee As Self* and *Contingent Worker As Self* for the Approve and Deny actions in the **Who Can Do Actions on Entire Business Process** section.
   g. Click **OK**.
4. Activate your security policy changes.
   a. Access the **Activate Pending Security Policy Changes** task.
   b. Enter *Enabling users to request proxy access, approve or deny proxy access requests, and view notifications about policy changes* in the **Comment** field.
   c. Click **OK**.
   d. Select the **Confirm** check box.
   e. Click **OK**.
5. Configure the *Constrained User Proxy* business process to route to users for their approval.
   a. Select the **My Proxy Dashboard** worklet on the Home page.
   b. Access the **Create Business Process Definition (Default Definition)** task.
   c. Select *Constrained User Proxy* from the **Business Process Type** prompt.
   d. Click **OK**.
   e. Add an *Approval* step to the business process definition.
   f. Enter the letter *b* in the **Order** field.
   g. Select *Approval* in the **Type** field.
   h. Select *Employee As Self* and *Contingent Worker As Self* in the **Group** field.
   i. Click **OK**.

6. Configure the *Termination* business process to revoke proxy policies from terminated workers.
    a. From the related actions menu of the *Termination* business process definition, select **Business Process** > **Edit Definition**.
    b. Click **OK**.
    c. Add a *Service* step to the business process definition.
    d. Enter the letters *bb* in the **Order** field.
    e. Select *Service* in the **Type** field.
    f. Select *Revoke Constrained Proxy Policies* from the **Specify** prompt.
    g. Click **OK**.

Next Steps

The assistant can request proxy access using the **Request Proxy Access** task and select the:

- CFO as the user to act on behalf of.
- *Report for Budget and Actual by Revenue Category* restriction set.
- End of their access as a week from the current date.

When the assistant completes the task, Workday notifies the CFO to approve or deny the request. If the CFO approves the request, the assistant can access the **Budget vs. Actual by Revenue Category** report using the **Start User Proxy** task on the **My Proxy Dashboard** worklet.

Related Information
Tasks
Steps: Set Up Constrained Proxy Access on page 211

Security for Integrations

Concept: Integration Security in Workday

The Workday security model for integrations consists of:

- *Access to systems and output*: Workday provides several security domains that secure access to integration templates and integration systems. These domains separate the permissions to configure an integration from the permissions to run an integration and view integration output. Example: Workday displays launch parameter prompt options based on the security permissions of the person configuring the integration, rather than the security permissions of the *Integration System User* (ISU) account that runs the integration. You can also segment integration templates and integrations, then grant access separately for each segment.
- *Access to Workday data*: All integrations access Workday data using web service operations, Reports-as-a-Service, or a Data Initialization Service (DIS). Workday secures these items to various security domains:
    - Web service operations.
    - Report data sources.
    - Report fields.
    - Custom reports.

    Integrations and applications that access Workday must have *Get* and *Put* access to the domains that include the web service operations. Also, they must have the appropriate (View) access to the domains

that include the report data sources and report fields. Outbound EIBs also require access to the custom report that they use as a data source. These accounts can control permissions:

- Associated ISU accounts (for Connectors, Studio integrations, and external applications).
- The person who runs the integration (EIB only).

- *Access to external endpoints*: Workday provides encryption, decryption, and signature options using PGP. Workday provides encryption (for AS2), SFTP authentication, SAML Logout, and web service authentication using X.509.

Access to Systems and Output

Steps: Secure Integrations by Segment

Prerequisites

- Create security groups for users.
- If you're setting up access to a specific integration system (rather than an integration template), create the integration first.

Context

Create an integration system security segment that contains 1 or more integration templates, integrations, or categories. Then create a segment-based security group that ties a security group to the integration segment. With integration-related security domains, you can separate the permissions to build an integration system from the permissions to view the integration output documents by template, integration, and category.

You can further secure integration systems by role. You can associate the integration process event for an integration system with a specific organization in Workday. Then you can associate the integration system segment to a role-based security group in a segment-based security group. Then you can grant the segment-based security group access to the *Integration Event* domain. As a result, group members can only see output documents for that integration system.

Steps

1. Access the **Create Integration System Security Segment** task and select the integration templates, integration systems, or category that you want to include in the segment.
2. Create Segment-Based Security Groups on page 185
   Select 1 or more security segments that you created in Step 1 from the **Access to Segments** prompt.
3. Edit Domain Security Policies on page 200.
   Grant appropriate permissions to the security groups that you created in Step 2.

Related Information

Concepts

Concept: Integration Business Processes

Tasks

Create Segment-Based Security Groups

Steps: Secure Message Queues by Segment

Prerequisites

- Identify an account whose credentials you want used by an external endpoint when accessing your Message Queues.
- Create 1 or more Message Queues in Workday (using Workday Studio) for your Studio integrations.

Context

Create a Message Queue security segment that contains 1 or more Message Queues, then create a segment-based security group that ties a security group to the integration segment.

Workday provides Message Queue security segments to enable you to apply finer control to who can access a Message Queue.

Steps

1. Create a Message Queue security segment:
   a) Access the **Create Message Queue Security Segment** task.
   b) Select 1 or more Message Queues that you want to include in the segment.
2. Create Segment-Based Security Groups on page 185.
   Select 1 or more security segments that you created in Step 1 from the **Access to Segments** prompt.
3. Edit Domain Security Policies on page 200.
   Grant access to the Segment-Based Security group you created in Step 2 to the *Message Queue (segmented)* domain.

Access to Workday Data

Steps: Grant Integration or External Endpoint Access to Workday

Prerequisites

- Note the security domains that your integration must access:
  - Connectors: You can find a list of required domains in the setup documentation for each Connector.
  - Studio and externally-developed integrations: Your developer can provide a list of the web service tasks used by the integration. To view the domain that secures the web service tasks, use the **View Security for Securable Item** report.
  - Enterprise Interface Builder (EIB): You can view the data sources and web services for an EIB using the **View Integration System** report. View the domain that secures the web service task or report data source with the **View Security for Securable Item** report.
- Security:
  - *Security Configuration* and *Security Administration* domains in the System functional area.
  - *Integration Security* domain in the Integration functional area.

Context

To authenticate with Workday and access web services, each integration system (Connector, Studio, or external) requires one of these types of account:

- An integration system user (ISU) account. Assigning an ISU is generally the preferred method. For security reasons, Workday restricts each ISU to a single integration system. The ISU must have access to the web service operations that interact with the necessary data. The security group that includes the ISU must have *Put* and *Get* access to domains that contain the web service operations.
- An account for a worker in Workday. Workday enables you to use the account for a person. Use the account for a person for testing or when needed in a business process step for the integration. If you secure an integration with an ISU, changes to Workday user accounts won't affect normal processing of your integration.

Steps

1. Access the **Create Integration System User** task and configure a Workday account for the integration.
   - Keep the **Session Timeout Minutes** default value of zero to prevent session expiration. An expired session can cause the integration to stop before it successfully completes.
   - Select the **Do Not Allow UI Sessions** check box. This option prevents the integration system user from signing in to Workday through the UI.
2. Create Integration System Security Groups on page 155.
3. Edit Domain Security Policies on page 200.
4. Activate Pending Security Policy Changes on page 203.
5. Access the **View Integration System** report and access the Connector, Studio, or EIB integration.
6. Select **Workday Account** > **Edit** as a related action on the integration system.
7. On the **Edit Account for Integration System** task, select the **Workday Account** that you created in Step 1.
8. (Optional) In the **Global Preferences** area, select a preferred locale and display language for the ISU. These settings control what language Workday uses for the integration data. An outbound integration sends data in the preferred language and an inbound integration saves data in the preferred language. If you leave these fields blank, Workday uses the default locale and display language for integration data.
9. If the ISU will authenticate using user name and password, access the **Maintain Password Rules** task. Add the integration system user to the **System Users exempt from password expiration** field.

   To avoid integration errors caused by expired passwords, Workday recommends that you prevent Workday passwords from expiring.

Verify EIB Security Configuration

Prerequisites

Security: *Integration Build* domain in the Integration functional area.

Context

EIBs don't have their own independent security permissions. Instead, EIBs inherit the security permissions of the worker who launches the EIB, or schedules the EIB to run in the future. This inheritance enables scheduled EIBs to run even if the worker who scheduled the EIB isn't present.

Every EIB has 1 data source, which can be a Workday Web Service operation or custom report. In addition, inbound EIBs also have an associated web service Put operation that loads the data into Workday. The EIB must be able to access the data source and web service Put operations. To access data, the worker running the EIB must have the appropriate access to the security domains that secure the data source and web service operations.

Workday restricts access to Workday data further using contextual security. Example: If a worker can access only certain compensation grades. If the worker runs an outbound EIB based on the *Get Compensation Grades* web service operation, the EIB only outputs data for the same compensation grades.

Note: If you grant a security group *Get* or *Put* access to a domain, the group also has *View* and *Modify* access to reports and tasks in that domain.

Steps

1. Access the **View Integration System** report.
2. From the **Integration System** prompt, select your EIB.

   EIBs are in the *Integration* folder.

3. (Outbound EIBs only) Record the custom report or web service operation listed in the **Data Source** field.

   To obtain the correct data source, access the underlying data source for the custom report. In addition to a primary *business object*, each data source can contain 1 or more secondary business objects. Different domains can secure these secondary business objects and the primary business object. If the data source displays as text instead of a link, you don't have security access to the underlying report or web service.
4. (Inbound EIBs only) Record the web service operation listed in the **Workday Endpoint** field.
5. Access the **View Security for Securable Item** report.
6. Search for each web service and data source that you recorded in the preceding steps.
7. Record the security domain that secures each web service operation and data source.

   If the report displays a web service operation that doesn't have a domain listed, a business process secures the web service operation. Access the business process security policy for that business process and record the domain.
8. Ensure that you're a member of a security group that has the following access to the domains that you've recorded:
   - View permissions to any custom report that you select.
   - Put access to the domain securing any web service that you select for an inbound EIB.
   - Get access to the domain securing any web service that you select for an outbound EIB.

Related Information
Tasks
Edit Domain Security Policies

Verify Authorization Security for Workday Web Services

Prerequisites

This task requires some technical familiarity with web service conventions.

Security: *Security Administration* domain in the System functional area.

Context

To ensure that your external application can use the Workday Web Services (WWS) API to access Workday:

- Review the WWS API documentation.
- Record every web service operation that your application invokes.
- Verify that the application account has access to the domain that secures the web service operations.

If you grant a security group *Get* access to a domain, the group also has *View* access to reports and tasks in that domain. If you grant a security group *Put* access to a domain, the group also has *View and Modify* access to reports and tasks in that domain.

Steps

1. Access the Workday Web Services API Documentation on the Workday Community.
2. For each web service, record the web service operations that your application will use.
3. For each element in each web service operation, review the parameters list for subelements that domains separate from the parent element secure. Record the domain listed in the Security Note:

   Security Note: This element is secured according to the security policy for the <name of security domain> domain.
4. Access the **View Security for Securable Item** report.

5. Search for each web service operation that you recorded in the preceding steps. Then, record the security domain that secures each web service operation.

   If the report displays a web service operation that doesn't have a domain listed, a business process secures the web service operation. Access the business process security policy for that business process and record the domain.
6. Add the account that your application uses for access to a security group with *Get* or *Put* access to the domains containing the web services.

Related Information
Tasks
Edit Domain Security Policies

Access to External Endpoints

Create an X.509 Public Key

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

Upload public X.509 certificates to Workday for use with the AS2 transport protocol, SAML authentication, and web service token authentication.

Steps

1. Retrieve the X.509 public key certificate text from your external server or partner.

   The certificate must be in PEM format.
2. Access the **Create x509 Public Key** task.
3. Paste the X.509 public key certificate text from your external partner in the **Certificate** field.

   Start the text with: `-----BEGIN CERTIFICATE-----`.

   End the text with: `-----END CERTIFICATE-----`.

Create an X.509 Private Key Pair

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

Create X.509 private key pair certificates (in RSA 2048-bit format) for use with the AS2 transport protocol, SFTP key authentication, and SAML authentication.

Workday recommends that you create the private key pair in your Production tenant. If you create a key in a non-Production tenant, you won't be able to migrate it to Production. Workday refreshes your Sandbox tenant from your Production tenant during the Weekly Service Update. Your external trading partner won’t need to use a new public key every week.

X.509 private key pairs have built-in expiration dates. Workday displays the expiration date in the **Valid To** field of the **View x509 Private Key Pair** report.

Steps

1. Access the **Create x509 Private Key Pair** task and generate a public key and corresponding private key. You can optionally select the **Do Not Allow Regeneration** check box if you want to disable the regeneration of the key pair.
   When completed, this task displays the public key certificate text, divided into 2 sections.
2. Copy the relevant section of the public key and forward it to your external partner:
   - **Public Key**: Use for AS2 signature and SAML logout.
   - **RSA-SSH Formatted Key**: Use for SFTP key authentication.

     Note:

     Workday displays the RSA-SSH public key (SSH2 format). If the external server requires the *openSSH* format, convert the RSA-SSH public key using an external tool. To convert your SSH2 key to *openSSH*, use 1 of these tools:

     - https://burnz.wordpress.com/2007/12/14/ssh-convert-openssh-to-ssh2-and-vise-versa/
     - https://dev.to/itsopensource/conversion-of-ssh2-private-key-to-openssh-format-using-puttygen-3i70

Result

Workday stores the corresponding private key certificate. You can refer to the private key, but can't view the actual private key certificate text.

Next Steps

Regenerate your X.509 private key pairs before their expiration date to prevent integration processing issues.

Related Information

Tasks

Regenerate an Expired X.509 Private Key Pair on page 225

Create a Third-Party X.509 Key Pair

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

You can save X.509 key pairs supplied by a third-party certificate authority to Workday. Example: When you implement an Affordable Care Act Information Returns (AIR) connector integration with the IRS.

Note: You can't use third-party X.509 key pairs for SAML SSO links or other places in Workday where you typically use X.509 keys.

Steps

1. Obtain the certificate information from your third-party certificate authority.
   If the private key that you obtained isn't in PKCS8 format, you need to convert it to that format.
2. Access the **Create 3rd Party X509 Key Pair** task.
3. As you complete the task, consider:

Option	Description
Certificate Text	The certificate: • Must not be expired. • Must be PEM encoded.

Option	Description
	• Can only be one public certificate, not a certificate chain. • Must include the certificate header and footer, including all of the dash (-) characters. Example: Select everything including -----*BEGIN CERTIFICATE*----- and -----*END CERTIFICATE*-----. Workday automatically checks for certificate validity.

Private Key	The private key:
	• Must be in PKCS8 format.
	• Must be PEM encoded.
	• Must not include extraneous characters such as newline characters.
	• Must include the private key header and footer, including all of the dash (-) characters. Examples: Select everything including:
	  • -----*BEGIN ENCRYPTED PRIVATE KEY*----- and -----*END ENCRYPTED PRIVATE KEY*-----.
	  • -----*BEGIN PRIVATE KEY*----- and -----*END PRIVATE KEY*-----.

Private Key Passphrase	The passphrase that the third-party certificate authority provides with an encrypted private key.

Regenerate an Expired X.509 Private Key Pair

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

X.509 private key pairs have built-in expiration dates. Workday displays the expiration date in the **Valid To** field of the **View x509 Private Key Pair** report. Regenerate your x509 private key pairs before they expire, to ensure that these types of processes continue to complete successfully:

- Integrations that use the AS2 transport protocol.
- Integrations that use the SFTP transport protocol.
- SAML authentication.
- Solutions migration.

Steps

1. Access the **View x509 Private Key Pair** report and select your X.509 private key pair from the **Private Key for Signature** prompt.
2. As a related action on the X.509 private key pair, select **x509 Private Key Pair** > **Regenerate Key Pair**.
3. Select **Confirm**.

   Copy the relevant section of the new public key and forward it to your external partner.

Load Externally Generated Private Key into Workday

Prerequisites

- Security: *Security Administration* domain in System functional area.
- Generate a Private Key from Google Cloud Storage.

Context

Load an externally generated RSA X.509 private key into Workday using the **Create Private Key** task.

Note: Only use this task for authentication with Google Cloud Storage (GCS). GCS requires you to generate an RSA X.509 Private Key *outside* of your Workday tenant. Otherwise, use the **Create x509 Private Key Pair** task, which generates the Private Key in Workday.

Steps

1. Retrieve the RSA X.509 Private Key certificate from your external server.
   The certificate must be in PEM format and have the *.pem* extension.
2. Access the **Create Private Key** task.
3. Paste the RSA Private Key text from the certificate into the **PEM Encoded Private Key** field.
   The text must begin with: `--- BEGIN RSA PRIVATE KEY ---`
   The text must end with: `--- END RSA PRIVATE KEY ---`

Create a PGP Public Key

Prerequisites

Ensure that the PGP certificate that your vendor provides is self-signed using SHA-256.

Security: *Security Administration* domain in the System functional area.

Context

Upload public certificates and associate certificates with integration systems that encrypt and sign data for inbound and outbound data integrations with your trading partners.

Steps

1. Retrieve the PGP public key certificate text from your external partner.
2. Access the **Create PGP Public Key** task.
3. Paste the PGP public key certificate text from your external partner in the **Certificate** field.

Example

In this scenario, you want to load a PGP public key certificate into Workday. Your trading partner, Acme Inc., has emailed you this PGP public key:

```
-----BEGIN PGP PUBLIC KEY BLOCK----- Version: PGPfreeware
6.5.8 for non-commercial use <http://www.pgp.com>
mQGiBDp1yy0RBADVlyDewVwltBs7HnHCG3bXlVUODFkn/00TdbM2SPnOAIkj4giB
ylOP7Mg+Hr5y7FIBvmPWx06In6JjNQiSbpshP5YHv57UfE79nEJdWuSTQt/7j7IJ
GkHYtBRHQMIAHMgT8IB5d3gFq52jSa8hw/ixMP09a0Rw8RP9+kOE4s9UrQCg/zVH
IHswdc/mb50PjdeXwnjxQbkD/3lJYEzz8eUlFHB4rVaC1yRi21Lypf0DIMfQg5j9
xBxY4odFJKyf22PeuAjp9roURRIbGIkIGH8eXF+Mav9OqEdD80JbEn1hZuaLk1RF
k1XJjmFRdKXz+Q7JmRdbs3zXXav2cYwalgzEXT5kuXuNlThLTnLoEFop8Hl3xM4/
PdqMBACkkHb07vPY5l429tdXqL00lE6LedlBW4FLjI534QgselsrUxq5U5y0Wg1Z //
```

```
a66l5QkyaMrpsHKfkLHdaPOVCs/WeG6eLwD/cUBEM1Y9Yb5DaB0njdZB3Yxcm8
W23hpKjDanb7SbaSA16gBIWRlvrB/qU+MZAj+EXRDJmwMJq2y7QjbmV0aXZhIGNh
ZnRvcmkgPG5ldGl2YWNAb25lYm94LmNvbT6JAE4EEBECAA4FAjp1yy0ECwMCAQIZ
AQAKCRDFpFclYzXzSwiRAJ0S3djCkJJPUalRyE+vWnfnhvJmDgCfTEBN2N6GlGWO
mrOg1tQlZoWbd5q5Ag0EOnXLLRAIAPZCV7cIfwgXcqK61qlC8wXo+VMROU+28W65
Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9Sh01D49Vlf3HZSTz09
jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brw
v0YAWCvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiN
jrtVjLhdONM0/XwXV0OjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrK
lQzZlp+r0ApQmwJG0wg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIH+wVFKD3A
FEdEBHqDZuKjLdLJIKHk4gloKeQ60R9NLLFynfIgSvgsii5uWLY9+gZ2FIGnP3Yc
GxZH1HASv+pG1sw0MnhutxZui3E3Mt69Uv1KTlTGYkfS+mXBw4Qr7hXavCkF45we
f/9Qlj6hSKVjy4YcewdvpopM9S4gVcBq+EdTp1negsCyj3YhFiEo0JEL40mnoHX7
HudJBbiBmknmBZOjxzBBeDPcu7fWV/LDCWiFoGg9uWy2KOcIt7sNXVJbukbSGYg2
hzOB2JPaqCqI5+4YfUCumNLd0lktT7S1V3/6xszEnybQL7tMtmrZZFAFHFAwLNPA
bLxdF/b26GbrTT+JAEYEGBECAAYFAjp1yy0ACgkQxaRXJWM180ttbQCg98c40J41
iXkP9CuqGR0LBJ46VNAAnj+5dH9N226fBp5TN0rAyxwBveTK =0VvA -----END PGP PUBLIC KEY
BLOCK-----
```

Use the **Create PGP Public Key** task to enter these values to create a public key for your tenant named *AcmeInc*:

Field	**Sample Value**
Name	*AcmeInc* **Note:** Workday uses the Name field to define the user ID (*uid*) of the PGP key pair.
Description	PGP Public Key provided by Acme, Inc.
Partner Certificate	[Selected]

Certificate	`-----BEGIN PGP PUBLIC KEY BLOCK-----`
	`Version: PGPfreeware 6.5.8 for non-commercial use <http://www.pgp.com>`
	`mQGiBDp1yy0RBADVlyDewVwltBs7HnHCG3bXlVUODFkn/00T`
	`ylOP7Mg`
	`+Hr5y7FIBvmPWx06In6JjNQiSbpshP5YHv57UfE79nEJdWuS`
	`GkHYtBRHQMIAHMgT8IB5d3gFq52jSa8hw/`
	`ixMP09a0Rw8RP9+kOE4s9UrQCg/zVH IHswdc/`
	`mb50PjdeXwnjxQbkD/3lJYEzz8eUlFHB4rVaC1yRi21Lypf0`
	`xBxY4odFJKyf22PeuAjp9roURRIbGIkIGH8eXF`
	`+Mav9OqEdD80JbEn1hZuaLk1RF`
	`k1XJjmFRdKXz`
	`+Q7JmRdbs3zXXav2cYwalgzEXT5kuXuNlThLTnLoEFop8Hl3`
	`PdqMBACkkHb07vPY5l429tdXqL00lE6LedlBW4FLjI534Qgs`
	`a66l5QkyaMrpsHKfkLHdaPOVCs/`
	`WeG6eLwD/cUBEM1Y9Yb5DaB0njdZB3Yxcm8`
	`W23hpKjDanb7SbaSA16gBIWRlvrB/qU`
	`+MZAj+EXRDJmwMJq2y7QjbmV0aXZhIGNh`
	`ZnRvcmkgPG5ldGl2YWNAb25lYm94LmNvbT6JAE4EEBECAA4FA`
	`AQAKCRDFpFclYzXzSwiRAJ0S3djCkJJPUalRyE`
	`+vWnfnhvJmDgCfTEBN2N6GlGWO`
	`mrOg1tQlZoWbd5q5Ag0EOnXLLRAIAPZCV7cIfwgXcqK61qlC8`
	`+VMROU+28W65`
	`Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ`
	`+AyDvWXpF9Sh01D49Vlf3HZSTz09`

Field	Sample Value
	jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/ xX5u/2RXscBqtNbno2gpXI61Brw v0YAWCvl9Ij9WE5J280gtJ3kkQc2azNsOA1FHQ98iLMcfFst ClWxiN jrtVjLhdONM0/ XwXV0OjHRhs3jMhLLUq/ zzhsSlAGBGNfISnCnLWhsQDGcgHKXrK lQzZlp+r0ApQmwJG0wg9ZqRdQZ +cfL2JSyIZJrqrol7DVekyCzsAAgIH+wVFKD3A FEdEBHqDZuKjLdLJIKHk4gloKeQ60R9NLLFynfIgSvgsii5u GxZH1HASv +pG1sw0MnhutxZui3E3Mt69Uv1KTlTGYkfS +mXBw4Qr7hXavCkF45we f/9Qlj6hSKVjy4YcewdvpopM9S4gVcBq +EdTp1negsCyj3YhFiEo0JEL40mnoHX7 HudJBbiBmknmBZOjxzBBeDPcu7fWV/ LDCWiFoGg9uWy2KOcIt7sNXVJbukbSGYg2 hzOB2JPaqCqI5+4YfUCumNLd0lktT7S1V3/6xszEnybQL7tM bLxdF/b26GbrTT +JAEYEGBECAAYFAjp1yy0ACgkQxaRXJWM180ttbQCg98c40J iXkP9CuqGR0LBJ46VNAAnj +5dH9N226fBp5TN0rAyxwBveTK =0VvA -----END PGP PUBLIC KEY BLOCK-----

You can now associate the *AcmeInc* public key with any outbound EIB or integration system that has Acme, Inc. as the trading partner. When Workday launches the outbound EIB or integration, the output files are encrypted with the public key that you loaded in this example. Acme, Inc. uses their corresponding private key to decrypt the integration files.

Create a PGP Private Key Pair

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

Create private key pairs for use with integration systems that encrypt and sign data for inbound and outbound data integrations with your trading partners.

Steps

1. Access the **Create PGP Private Key Pair** task and generate a public key and corresponding private key.
2. Copy the public key certificate text and forward it to your external partner.

   Workday stores the corresponding private key certificate; you can refer to the private key, but can't view the actual private key certificate text.

   If you create a private key pair in your Sandbox tenant, Workday removes the key during the next service update. You have to generate a new private key pair each week. In that case, your external trading partner must then reapply the public key every week. Workday recommends that you create the private key pair in your Production tenant. Workday copies the private key pair to your Sandbox tenant during the next service update.

Regenerate an Expired PGP Private Key Pair

Prerequisites

Security: *Security Configuration* domain in the System functional area.

Context

You can regenerate private PGP (Pretty Good Privacy) key pairs that encrypt and sign data in your inbound and outbound integrations.

PGP private key pairs have built-in expiration dates. Workday displays the expiration date in the **Valid To** field of the **View PGP Private Key Pair** report. Regenerate your PGP private key pairs before they expire to prevent integration processing issues.

Steps

1. Access the **View PGP Private Key Pair** report and select your key pair from the **PGP Private Key Pair** prompt.
2. As a related action on the PGP private key pair, select **PGP Private Key Pair** > **Regenerate Key Pair**.
3. Select **Confirm**.

   Copy the relevant section of the new public key and forward it to your external partner.

Related Information

Concepts

Concept: PGP Certificates in Workday on page 232

Set Up Workday Web Service Authentication

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

You can assign X.509 public keys or SAML tokens to integration system user accounts that authenticate and control access to web service requests directed to Workday. Inbound web service requests present authentication credentials that match credentials assigned to an integration system user. Then Workday enables authenticated web service requests to execute any *Get* and *Put* operations enabled by the security profile of the integration system user.

Steps

1. Access the **Configure Web Service Security** task.
2. From the **Integration System User** prompt, select the user whose security profile you want web service requests to use when accessing Workday.
3. To enable RSA-based authentication for your web service requests, select an **x509 Public Key** that verifies the signature on inbound web service requests.

   If you create a certificate, provide a name for the certificate in Workday and paste in the certificate information.
4. To enable SAML authentication for your web service requests, enter **SAML Token Configuration** settings:

Option	Description
SAML Identity Provider	Enter the Issuer value for your Identity Provider. This value must match the value of the Issuer element in the incoming SAML assertion.

Option	Description
Identity Provider's Public Key	Select an X.509 public key that verifies the signature on SAML sign-in and sign out requests. If you create a certificate, provide a name for the certificate in Workday and paste in the certificate information provided by the SAML identity provider. For a sample certificate, see: workday_pubkey.txt
Holder-of-Key's Public Key	(Optional) Select the X.509 public key for the key holder to verify the signature on SAML sign-in and sign out requests. If you create a certificate, provide a name for the certificate in Workday and paste in the certificate information provided by the SAML identity provider. For a sample certificate, see: workday_pubkey.txt

Example

For an example of setting up X.509 authentication for web service requests, see NET Utility for x.509 Workday Web Services Authentication.

Concept: X.509 Certificates in Workday

Workday supports the use of X.509 certificates for:

- AS2 file transport protocol: Workday encrypts and digitally signs outbound files sent using AS2 with X.509 certificates.
- SFTP and SAML authentication: Workday can exchange authentication credentials with external endpoints using X.509-based RSA certificates.
- Google Cloud Storage authentication: Workday can present an X.509-based RSA certificate to access a specific Google Cloud Storage bucket.
- Affordable Care Act Information Returns (AIR) connector integration: Workday uses X.509 certificates supplied by a third-party certificate authority to generate X.509 keys in your tenant. You can use these keys when implementing an AIR connector integration with the IRS.

You store all X.509 keys in your tenant. Storing keys in your tenant enables and requires that you maintain your own keys to ensure that you and your trading partners can secure your integration traffic.

Workday periodically scans for certificates that expire in 30, 15, 7, or less than 7 days and generates an email notification with details about any expiring certificates. To receive these notifications:

- Select the **Enable Security Emails** check box on the **Edit Tenant Setup - Security** task.
- You must have a valid work email address in your Workday contact information.
- You must have Modify permission on the *Security Administration* domain.

X.509 for Encryption

An X.509 certificate consists of a public key/private key pair. You can use this key pair for:

- Data encryption. The intended recipient creates an X.509 certificate. The recipient then shares the public key of the X.509 certificate with the sender of the file. The sender uses the public key to encrypt the outbound file. The recipient then uses the private key of the X.509 certificate to decrypt the inbound file.

- Digital signatures. The sender of the signed file creates an X.509 certificate. The sender then shares the public key of the X.509 certificate with the recipient. The sender uses the private and public key of the X.509 certificate to create the digital signature. The sender shares the public key of the X.509 certificate with the recipient of the file. The public key verifies the digital signature.

AS2 File Transport Protocol Encryption and Digital Signatures

You can configure your outbound integrations that use the AS2 file transport protocol to send encrypted and digitally signed files. Your trading partner must generate an X.509 certificate and send you the public key. You then load the public keys from the trading partner into your Workday tenant and associate it with the file transport protocol for a Connector or EIB. You also must create a separate X.509 private key pair in Workday and associate it with the file transport protocol for the Connector or EIB. Then send the corresponding Public Key portion of the certificate to your trading partner.

When you launch the integration, Workday uses the associated X.509 public key to encrypt and the X.509 private key pair to sign the integration file digitally. Your trading partner can decrypt the file using the private key that corresponds to the public key used on the file. Your trading partner can verify the digital signature using the public key associated to the X.509 private key pair.

X.509 for Authentication

For authentication credential encryption and decryption, Workday supports RSA. RSA uses the X.509 standard, a public key infrastructure (PKI) for Single Sign-On (SSO) and Privilege Management Infrastructure (PMI). The X.509 standard provides an asymmetric key encryption scheme; each entity has a key pair, and each pair consists of 1 public key and 1 private key. The public key encrypts authentication credentials and the corresponding private key enables you to decrypt those credentials. You provide the public key to entities that encrypt credentials only for you, so distributing your public key isn't a security concern. Your private key secures data encrypted with your public key.

Authentication Credential Encryption and Decryption

You can configure your outbound integrations to provide RSA authentication credentials to the file server of your trading partner. You must use the **Create X509 Private Key Pair** task to generate a private key pair. You then send the RSA-SSH Formatted Key portion of the certificate to your trading partner. Workday only generates X.509 private key pairs using RSA-2048. You can generate RSA-4096 private key pairs using third-party applications. Example: Putty. However, Workday only recommends using the RSA-2048 private key pairs that you generate with the **Create X509 Private Key Pair** task in your integrations. In situations where regenerating in-use key pairs can have negative consequences, such as with certain integrations, you can prohibit regeneration. Select the **Do Not Allow Regeneration** check box on the **Create x509 Private Key Pair** task when you generate the private key pair.

Note: For AIR connector integrations, you can use the **Create 3rd Party X.509 Key Pairs** task to generate key pairs using certificate information from a third-party certificate authority.

When you launch the outbound integration, Workday uses the RSA private key to provide authentication credentials to your trading partner file server. Your trading partner can verify the credentials using the public key that corresponds to the private key. This verification ensures that you're the party providing the authentication credentials.

You can configure your inbound integrations to accept RSA authentication credentials provided by your trading partner. You must get an RSA public key from your trading partner. You then associate the public key with the file transport protocol for a Connector or EIB.

When you launch the inbound integration, Workday uses the associated RSA public key to verify the authentication credentials from your trading partner.

Related Information
Tasks
Create an X.509 Private Key Pair on page 223

Create a Third-Party X.509 Key Pair on page 224
Regenerate an Expired X.509 Private Key Pair on page 225
Set Up Workday Web Service Authentication on page 229
Steps: Set Up Integration to Import Worker Time Card Data
Reference
Reference: Outbound Transport Protocol Types for EIBs

Concept: PGP Certificates in Workday

Workday can encrypt outbound and decrypt inbound Cloud Connect, Studio, and EIB (Enterprise Interface Builder) integration files using PGP (Pretty Good Privacy). Workday can also:

- Digitally sign your outbound integration files.
- Verify the signatures of your inbound integration files.

These options ensure that only you and your trading partners can read the data that you exchange. It also enables:

- Your trading partner to confirm that an outbound integration file comes from you.
- Workday to verify that an inbound integration file comes from you or your trading partner.

You store all PGP keys in your tenant. This action requires that you maintain your own encryption keys to ensure that you and your trading partners can secure your integration traffic.

Workday periodically scans for certificates that expire in 30, 15, 7, or fewer than 7 days. It generates email notifications about any expiring certificates. To receive these notifications:

- Select the **Enable Security Emails** check box on the **Edit Tenant Setup - Security** task.
- You must have a valid work email address in your Workday contact information.
- You must have Modify permission on the *Security Administration* domain.

About PGP

For data encryption and signing, Workday supports PGP, a public key encryption standard. PGP provides an asymmetric key encryption scheme; each entity has a key pair, and each pair consists of 1 public key and 1 private key. Trading partners use the public key to encrypt data and verify digital signatures. They use the corresponding private to sign files and decrypt data. You provide the public key to entities that encrypt data only for you, so distributing your public key isn't a security concern. Other parties can decrypt data encrypted with your public key only with your private key.

Depending on your integration needs, you can encrypt and sometimes sign outbound files, and decrypt incoming files. All of these operations require you to exchange and use different combinations of PGP public and private key certificates with external services. Each integration system requires 1 PGP key pair to encrypt a file, and an additional PGP key pair to sign the file. You might need to manage multiple pairs of PGP certificates with each external service. This table summarizes who does what with public and private keys.

Feature	How it Works
PGP Encryption (Outbound)	Workday's recipient creates a key pair, gives Workday the public key, and uses the private key to decrypt the file. Workday uses the public key to encrypt the outbound file. Workday's recipient uses the private key to decrypt the file.
PGP Signature (Outbound)	Workday's customer creates a key pair, gives the public key to their recipient, and uses the private key to sign the outbound file. The recipient uses

Feature	How it Works
	the public key to verify that the file came from Workday's customer and not someone else.
PGP Decryption (Inbound)	Workday's customer creates a key pair, gives the public key to the sender of the inbound file, and uses the private key to decrypt the inbound file. The sender uses the public key to encrypt the inbound file.
PGP Signature Verification (Inbound)	Workday's customer creates a key pair, gives the public key to Workday, and uses the private key to sign the file. Workday uses the public key to verify that the file came from the sender of the inbound file and not someone else.

PGP Version Support and Background

Workday uses an *OpenPGP* compatible cryptographic library that supports PGP 5.0 and later. The major split in PGP versions occurs between versions before PGP 5.0 and versions after PGP 5.0. After the release of PGP 5.0, the IETF *OpenPGP* standard (RFC 4880) was introduced. Since then, PGP standards have complied with that RFC.

Workday uses a Bouncy Castle library that is a full implementation of the *OpenPGP* specification. Workday is compatible with PGP 5.0 and later as provided by suppliers in compliance with the RFC. In other words, Workday is compatible with third-party software (other than PGP products) that use the *OpenPGP* encrypted standard.

Before PGP 5.0, a widely used version was PGP 2.6.x. Various suppliers supported this version, leading to several variants of PGP 2.6.x. None of these versions remain in common use today. However, it’s possible that some late adopters of PGP haven’t upgraded their PGP software in many years, and are still using a type of PGP 2.6.x. Although Workday doesn't support PGP 2.6.x, Workday has addressed the potential for integrating with these environments. Workday designed the current approach to PGP encryption so that it duplicates the logic that was in older Workday/PGP integrations. Workday has also tested this approach with older PGP integrations and has found no significant issues.

Integration File Encryption

You can configure your outbound Integration Cloud Connect and EIB integrations to send encrypted files that only your trading partner can decrypt. Your trading partner must generate a public key and corresponding private key, and send you the public key. You then load the public key into your Workday tenant, associate it with an Integration Cloud Connect or EIB integration, and specify:

- The name of the file when decrypted.
- The file format (PGP or ASCII Armored).
- Whether to include a message integrity check in the file.
- Whether the file is compatible with PGP 2.6.x and earlier formats.

When you launch the integration, Workday uses the associated PGP public key to encrypt the file and applies the output options. Your trading partner can decrypt the file using the private key that corresponds to the public key used on the file. Encryption ensures that if outside parties intercept the integration file in transit, they’re unable to read the contents.

Integration File Decryption

You can configure inbound Integration Cloud Connect and EIB integrations to decrypt files that your trading partner has encrypted. Generate a PGP private key pair in Workday, and send the public key to

your trading partner. You then associate the private key pair with an Integration Cloud Connect or EIB integration.

When you launch the integration, Workday uses the associated PGP private key to decrypt the inbound file.

Digital Signatures

You can configure your outbound Integration Cloud Connect and EIB integrations to apply a digital signature to encrypted integration files. You can also configure Workday to validate the signature when it decrypts inbound integration files.

To sign an integration file digitally, you generate a private key and matching public key (a key pair) in Workday. You provide the public key to your trading partner; the private key remains in your Workday tenant. You then associate the key pair with an outbound Integration Cloud Connect or EIB integration system. When you launch an outbound Integration Cloud Connect or EIB integration, Workday signs the integration file by applying the private key to the integration file. When your trading partner receives the integration file, the public key that you provided to the trading partner matches the private key on the file itself. The matching keys verify that the file came from your Workday tenant, and not from another party.

To verify a digital signature, you select the public key that your trading partner provides to you. When you launch an inbound integration, Workday applies the public key of the integration file to verify that the inbound file came from your trading partner.

Note: You can only apply digital signatures and integrity checks to encrypted integration files.

Using PGP Keys

You can create a separate public key and private key pair for each Integration Cloud Connect integration and EIB. For each integration that you want to encrypt and sign with PGP, you associate a public key or private key pair with that integration or EIB:

- **Integration Cloud Connect integration**: You configure the integration delivery to associate public and private keys and specify output options.
- **Inbound EIB integration**: When creating or editing an EIB, you create a File Transfer Protocol. Associate that File Transfer Protocol with an External File Data Source and the private key pair. Then use that External File Data Source as the data source for the EIB.
- **Outbound EIB integration**: When creating or editing an outbound EIB, you specify the PGP public key as part of the delivery options.

Related Information
Tasks
Set Up Inbound EIB
Set Up Outbound EIB
Set Up Integration Retrieval
Set Up Integration Delivery

Reference: X.509 Authentication Supported Algorithms

Workday enables you to make web service requests using X.509 Token Authentication.

Workday supports these algorithms for X.509 authentication.

Digest

Method	URI	Supported?
SHA256	http://www.w3.org/2001/04/xmlenc#sha256	Yes

Method	URI	Supported?
SHA512	http://www.w3.org/2001/04/xmlenc#sha512	Yes
SHA1	http://www.w3.org/2000/09/xmldsig#sha1	No
RIPEMD160	http://www.w3.org/2001/04/xmlenc#ripemd160	No

The digest value must be the hashed result of the entire SOAP envelope.

Signature

Method	URI	Supported?
RSA_SHA256	http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	Yes
RSA_SHA1	http://www.w3.org/2000/09/xmldsig#rsa-sha1	Yes
DSA_SHA1	http://www.w3.org/2000/09/xmldsig#dsa-sha1	No
HMAC_SHA1	http://www.w3.org/2000/09/xmldsig#hmac-sha1	No

The signature value must be the signed result of the Signed Info element.

Transform

Method	URI	Supported?
ENVELOPED	http://www.w3.org/2000/09/xmldsig#enveloped-signature	Yes
BASE64	http://www.w3.org/2000/09/xmldsig#base64	No
XPATH	http://www.w3.org/TR/1999/REC-xpath-19991116	No
XPATH2	http://www.w3.org/2002/06/xmldsig-filter2	No
XSLT	http://www.w3.org/TR/1999/REC-xslt-19991116	No

Canonicalization

Method	URI	Supported?
INCLUSIVE	http://www.w3.org/TR/2001/REC-xml-c14n-20010315	Yes
INCLUSIVE_WITH_COMMENTS	http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments	Yes

Method	URI	Supported?
EXCLUSIVE	http://www.w3.org/2001/10/xml-exc-c14n	Yes
EXCLUSIVE_WITH_COMMENTS	http://www.w3.org/2001/10/xml-exc-c14n#WithComments	Yes

Example

```
<soapenv:Envelope xmlns:bsvc="urn:com.workday/bsvc" xmlns:soapenv="http://
schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Header>
    <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/
oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <wsse:UsernameToken wsu:Id="UsernameToken-20" xmlns:wsu="http://
docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
utility-1.0.xsd">
        <wsse:Username>username@tenant</wsse:Username>
      </wsse:UsernameToken>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-
exc-c14n#" />
          <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-
more#rsa-sha256" />
          <Reference URI="">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/
xmldsig#enveloped-signature" />
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2001/04/
xmlenc#sha256" />
            <DigestValue>7D+kLj99X5qrGjCOUbGbaUHp0aKYpYUoHSxyCKoC6SY=</
DigestValue>
          </Reference>
        </SignedInfo>
        <SignatureValue>SiJilbvlC1p+ERraCG/
MqH3AylnRsfNqQpq4v8BpwMRCik6l0YSIhG8x2QpHwIAR
+sCnOLGp1FV8eQmvKWbgTfVgjShCk3uRKdYZnWmD5WiKUW3ADn7GjvtMhw6yvIKHW
        E4oLVpQpXfKYBSfVa3xKmkFABaeDSaCo/
daIQDCHj4j86geNUsKHTzFaz7W2GsyD2103RbBvkpz/udjRtALxtYKMhm/
+Vt60rjdYQL15E8fBivzZOm4Cg7Lio1DMcgR82ikO4WPJe2aJXBepvr
        KNEKAEno5QCULGgQj6uqCwDSg0vPtvJCc4IA5jSXLib/iMNPP8FFuvDBCj2EfpZ/
QiA==</SignatureValue>
        <KeyInfo>
          <X509Data>
            <X509Certificate>MIIC0jCCAbqgAwIBAgIQJXcd3k5+XoFE9Hd
+yXWPyjANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdra3VvLTAxMB4XDTExMDYwNzIzMTM1MloXDTEyMDYwNzA
wqXCPiwb1oF3MMFhBDd+vIcOEtmfG3k5GOtfE
+23vyA1kQWV2WXxQIGYORybiHi6tB4Usqi3fORyrfVXBbqSk4dT23KEN
+lNxfMvsn8fDa1VqoxFDA4EqlzhkeoawuYBg3KAaZCu808KMwdQYEgz78vA
+yCUO2DI97b4Zm28aSKgkpIOFRKx7k8RZ8tXKGqA6mTyq5pDW
+JhqdMhDpOKnRFV2vePNs2OTRww9QfR227VhNeb3N
+hRuGwD79dT85pBfcxb6xpTUQECAwEAAaMkMCIwCwYDVR0PBAQDAgQwMBMGA1UdJQQMMAoGCCsGAQUFBwMBMA0G
++jZ8xh+7sapNgVsKg2X9w76jDa1I
+CDKpWA9rTQ92e82rupGdHqX31cWzGb5Z3VpLGjFfSyUI0wP7Lu8G/
fjQtL48A9lNDOnd7LDzhz7U14wfqhj4hZQtqD75Y8gbi3+BG9jQBby8ORFWln64O4SzbDmN8/
HfmmjRsquHFDZB7LoaM0x8fpjTfCSz4OwhqRw02QGjQpvCw/hXEIIsuOsGx
+Y83bwAkPNh1wAn6CV56gCIwmRROnqUTPoW334UlblfwSjpgxddKDwlsgm61UtN5kNzqLEDwAbelZD1ujuFXZtbv
+Q08LGcXnDVi1s1eC</X509Certificate>
          </X509Data>
```

```
        </KeyInfo>
      </Signature>
    </wsse:Security>
  </soapenv:Header>
  <soapenv:Body>
    <wd:Get_Workers_Request xmlns:wd="urn:com.workday/bsvc">
      <wd:Response_Filter>
        <wd:Page>1</wd:Page>
        <wd:Count>1</wd:Count>
      </wd:Response_Filter>
    </wd:Get_Workers_Request>
  </soapenv:Body>
</soapenv:Envelope>
7D+kLj99X5qrGjCOUbGbaUHp0aKYpYUoHSxyCKoC6SY=
SiJilbvlC1p+ERraCG/MqH3AylnRsfNqQpq4v8BpwMRCik6l0YSIhG8x2QpHwIAR
+sCnOLGp1FV8eQmvKWbgTfVgjShCk3u
RKdYZnWmD5WiKUW3ADn7GjvtMhw6yvIKHWE4oLVpQpXfKYBSfVa3xKmkFABaeDSaCo/
daIQDCHj4j86geNUsKHTzFaz7W2G
syD2103RbBvkpz/udjRtALxtYKMhm/
+Vt60rjdYQL15E8fBivzZOm4Cg7Lio1DMcgR82ikO4WPJe2aJXBepvrKNEKAEno5QCULGg
Qj6uqCwDSg0vPtvJCc4IA5jSXLib/iMNPP8FFuvDBCj2EfpZ/QiA==

   MIIC0jCCAbqgAwIBAgIQJXcd3k5+XoFE9Hd
+yXWPyjANBgkqhkiG9w0BAQUFADASMRAwDgYDVQQDEwdra3VvLTAxMB4XDTE
xMDYwNzIzMTM1MloXDTEyMDYwNzAwMDAwMFowEjEQMA4GA1UEAxMHa2t1by0wMTCCASIwDQYJKoZIhvcNAQEBBQA
CCAQoCggEBAIsKSmvoynnbjYaG96po5imzg9Tf7Nnq26lE7gRqpckyGiUkEOjkMAcWcS2m6UqdOAoC6IoHpD/
wqXCPiwb1oF3MMFh
BDd+vIcOEtmfG3k5GOtfE
+23vyA1kQWV2WXxQIGYORybiHi6tB4Usqi3fORyrfVXBbqSk4dT23KEN
+lNxfMvsn8fDa1VqoxFDA4Eq
lzhkeoawuYBg3KAaZCu808KMwdQYEgz78vA
+yCUO2DI97b4Zm28aSKgkpIOFRKx7k8RZ8tXKGqA6mTyq5pDW+JhqdMhDpOKnRFV2ve
PNs2OTRww9QfR227VhNeb3N
+hRuGwD79dT85pBfcxb6xpTUQECAwEAAaMkMCIwCwYDVR0PBAQDAgQwMBMGA1UdJQQMMAoGCCsGAQUFB
wMBMA0GCSqGSIb3DQEBBQUAA4IBAQBKUxWRRkyzmge6LFUkgF++jZ8xh
+7sapNgVsKg2X9w76jDa1I+CDKpWA9rTQ92e82rupGdHqX
31cWzGb5Z3VpLGjFfSyUI0wP7Lu8G/
fjQtL48A9lNDOnd7LDzhz7U14wfqhj4hZQtqD75Y8gbi3+BG9jQBby8ORFWln64O4SzbDmN8
/HfmmjRsquHFDZB7LoaM0x8fpjTfCSz4OwhqRw02QGjQpvCw/hXEIIsuOsGx
+Y83bwAkPNh1wAn6CV56gCIwmRROnqUTPoW334Ulbl
fwSjpgxddKDwlsgm61UtN5kNzqLEDwAbelZD1ujuFXZtbvRd+Q08LGcXnDVi1s1eC
                                                  1         1
```

FAQ: Encryption, Certificates, and Ciphers for Integrations

Which key type do I need to use for my integration?

This table lists:

- The different encryption and authentication features available for use with Workday integrations.
- The certificate type that each encryption and authentication feature requires.

Feature	Workday Role	Type to Use
PGP Encryption (Outbound)	Sender	PGP Public Key
PGP Signature (Outbound)	Sender	PGP Private Key Pair

Feature	Workday Role	Type to Use
PGP Decryption (Inbound)	Recipient	PGP Private Key Pair
PGP Signature Verification (Inbound)	Not supported	None
AS2 Encryption (Outbound)	Sender	X.509 Public Key
AS2 Signature (Outbound)	Sender	X.509 Private Key Pair
AS2 Decryption/ Signature Verification	Not supported	None
Google Cloud Storage Authentication	Sender	X.509 Private Key from Google Cloud Storage account.
SFTP (SSH) Key Authentication	Sender and Recipient	X.509 Private Key Pair
SAML sign-in	Recipient	X.509 Public Key
SAML *IdP* Initiated Log Out Response	Sender	X.509 Private Key Pair
SAML Workday-Initiated Log Out Request	Sender	X.509 Private Key Pair
Web Service X.509 Token Authentication	Recipient	X.509 Public Key
ACA Integration Connector	Recipient	X.509 Third-Party Key Pair

Is encryption always required?

Integrations that use unencrypted transport protocols (email and FTP) often require PGP encryption. You can override this requirement for EIBs only (not Connectors).

Does Workday support decryption of inbound files sent by AS2?

No. Workday doesn't currently support AS2 decryption.

Which format can I use when sharing with an external service or vendor?

Integration Type	Workday Role	Key Type to Use	Public Key Format
AS2 Signature (Outbound)	Sender	X.509 Private Key Pair	Public Key
SFTP (SSH) Key Authentication	Sender and Recipient	X.509 Private Key Pair	RSA-SSH Formatted Key
SAML Logout	Sender	X.509 Private Key Pair	Public Key

Which types of encryption cipher can I use with Workday?

Workday supports these ciphers in its Document Delivery and Retrieval service. Workday also supports these ciphers in the SFTP-OUT component in Workday Studio:

- *3des-cbc*
- *3des-ctr*
- *aes128-cbc*
- *aes128-ctr*
- *aes192-cbc*
- *aes192-ctr*
- *aes256-cbc*
- *aes256-ctr*
- *arcfour*
- *arcfour128*
- *arcfour256*
- *blowfish-cbc*
- *blowfish-ctr*
- *cast128-cbc*
- *cast128-ctr*
- *idea-cbc*
- *idea-ctr*
- *None*
- *rsa-sha2-256* (SFTP server must be RFC-8308-compliant)
- *rsa-sha2-512* (SFTP server must be RFC-8308-compliant)
- *serpent128-cbc*
- *serpent128-ctr*
- *serpent192-cbc*
- *serpent192-ctr*
- *serpent256-cbc*
- *serpent256-ctr*
- *ssh-rsa* (SFTP server must be RFC-8308-compliant)
- *twofish192-cbc*
- *twofish192-ctr*

- *twofish256-cbc*
- *twofish256-ctr*
- *twofish-cbc*

Workday supports these ciphers on the SFTP-Out component in Workday Studio for assembly versions before 2020.09:

- *3des-cbc*
- *aes128-ctr*
- *aes192-ctr*
- *aes256-ctr*
- *blowfish-cbc*
- *None*

Note: For performance reasons, Workday recommends that you perform encryption on the Delivery service, rather than on the Workday Studio SFTP-Out component.

Which Transport Layer Security (TLS) version and cipher suites does Workday support for HTTP in Workday integrations?

Workday uses the Java Development Kit (JDK) 1.8 standards for TLS and cipher suites with the addition of SSLv3. Workday supports these TLS versions:

- Inbound integrations: TLS version 1.2 and later.
- Outbound integrations: TLS version 1.2 and later.

Workday enables these cipher suites by default:

- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_GCM_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_ECDSA_WITH_RC4_128_SHA

- TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDH_RSA_WITH_RC4_128_SHA
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_EMPTY_RENEGOTIATION_INFO_SCSV
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Workday disables these cipher suites by default:

- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_RSA_WITH_DES_CBC_SHA
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_RSA_WITH_NULL_MD5
- SSL_RSA_WITH_NULL_SHA
- TLS_DH_anon_WITH_AES_128_CBC_SHA
- TLS_DH_anon_WITH_AES_128_CBC_SHA256
- TLS_DH_anon_WITH_AES_128_GCM_SHA256

- TLS_DH_anon_WITH_AES_256_CBC_SHA
- TLS_DH_anon_WITH_AES_256_CBC_SHA256
- TLS_DH_anon_WITH_AES_256_GCM_SHA384
- TLS_ECDH_anon_WITH_3DES_EDE_CBC_SHA
- TLS_ECDH_anon_WITH_AES_128_CBC_SHA
- TLS_ECDH_anon_WITH_AES_256_CBC_SHA
- TLS_ECDH_anon_WITH_NULL_SHA
- TLS_ECDH_anon_WITH_RC4_128_SHA
- TLS_ECDH_ECDSA_WITH_NULL_SHA
- TLS_ECDH_RSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_KRB5_EXPORT_WITH_DES_CBC_40_MD5
- TLS_KRB5_EXPORT_WITH_DES_CBC_40_SHA
- TLS_KRB5_EXPORT_WITH_RC4_40_MD5
- TLS_KRB5_EXPORT_WITH_RC4_40_SHA
- TLS_KRB5_WITH_3DES_EDE_CBC_MD5
- TLS_KRB5_WITH_3DES_EDE_CBC_SHA
- TLS_KRB5_WITH_DES_CBC_MD5
- TLS_KRB5_WITH_DES_CBC_SHA
- TLS_KRB5_WITH_RC4_128_MD5
- TLS_KRB5_WITH_RC4_128_SHA
- TLS_RSA_WITH_NULL_SHA256

Note: Workday has decommissioned support for SHA-1, and longer supports these cipher suites for inbound integrations:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- SSL_CK_DES_192_EDE3_CBC_WITH_SHA

Which SFTP Key Exchange (KEX) algorithms does Workday support?

Workday supports these KEX algorithms:

- *diffie-hellman-group1-sha1*
- *diffie-hellman-group14-sha1*
- *diffie-hellman-group14-sha256*
- *diffie-hellman-group16-sha512*
- *diffie-hellman-group-exchange-sha1*
- *diffie-hellman-group-exchange-sha256*
- *ecdh-sha2-nistp256*
- *ecdh-sha2-nistp384*
- *ecdh-sha2-nistp521*

Which Server Host Key algorithms does Workday support?

Workday supports these server host key algorithms:

- *ecdh-sha2-nistp256*
- *ecdh-sha2-nistp384*
- *ecdh-sha2-nistp521*
- *rsa-sha2-256*
- *rsa-sha2-512*

	• *ssh-ed25519*
Which Message Authentication Code (MAC) algorithms does Workday support?	Workday supports these algorithms: • *hmac-md5* • *hmac-md5-96* • *hmac-sha1* • *hmac-sha1-96* • *hmac-sha2-256* • *hmac-sha2-256-96* • *hmac-sha2-512* • *hmac-sha2-512-96* • *None*

Accounts

Workday Accounts

Steps: Manage Passwords

Context

Set tenant-wide password rules and configure how users can reset or change their passwords. These steps don't apply to accounts managed by delegated authentication or third-party identity providers that rely on single-sign-on, such as SAML or OpenID. You must still manage passwords for accounts that sign in using passwordless sign-in, because users need to sign in to Workday with their password to set it up.

Steps

1. Define Password Rules on page 251.

   You can configure a set of password rules for users to process credit card information and another set for all other users in your tenant.
2. Manage Challenge Questions on page 32.

   Note: Workday plans to retire challenge questions in a future release.
3. Configure Password Reset on page 253.

Result

Users can:

- Reset or change their Workday password based on the conditions you set. When signed in, they can use the **Manage Security Settings** report to access the **Change Password** task.
- Use the **Manage Password Challenge Questions (Do Not Use)** task to configure their challenge questions or answers.

Example

This example illustrates how to set up Workday to enable users to reset forgotten passwords using a one-time use link that Workday sends to them in an email.

1. Define these password rule settings for the tenant on the **Maintain Password Rules** task. Other settings on the task are unimportant for this example:

Field	Setting
Minimum Password Length	8
Password Must Contain Alphabetic Characters	Selected
Password Must Contain Uppercase Characters	Selected
Password Must Contain Lowercase Characters	Not selected
Password Must Contain Numeric Digits	Selected
Password Must Contain Special Characters	Not selected

2. Define these security email settings for the tenant on the **Edit Tenant Setup - Security** task. Other settings on the task are unimportant for this example:

Field	Setting
Enable Security Emails	Selected, with **Send to work email, else home email** selected.
Enable Forgotten Password Reset	Selected, with **One-Time Use Link** selected.

Workday displays a **Forgot Password?** link on the sign-in page. To reset a user's password:

1. The user clicks the **Forgot Password?** link.
2. Workday displays a **Forgot Password** prompt.
3. The user enters their user name and primary Workday email address at the prompt.
4. Workday sends an email containing a reset password link to the user.
5. The user clicks the reset password link in the email.
6. At the **Change Password** prompt that displays, the user enters their new password, and then enters it again to verify it.

The user can now sign in using their new password. The password rules for this example require that the new password contain a minimum of 8 alphanumeric characters, with at least 1 uppercase character and 1 numeral.

Next Steps

You can access the **Edit Workday Account** task to manage password settings for individual Workday accounts.

Define Username Requirements

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

You can set up rules to specify how Workday constructs usernames for accounts that Workday manages. Once defined, the rules are in effect for all business processes that use the *Create Workday Account* service. These requirements don't apply to accounts managed by:

- Delegated authentication.
- Third-party identity providers that rely on Single Sign-On protocols, such as SAML or OpenID.

Usernames must be unique. You can create additional rules to resolve duplicate usernames. Workday recommends not basing your first rule on an optional attribute, such as a user's primary home email address. Optional attributes can return an empty value.

If the first rule in your rule group can't produce a unique username, Workday evaluates the next rule until it successfully produces one. If Workday evaluates all rules and can't create a unique username, it reevaluates the first rule. Then, if the first rule can produce a username but that username isn't unique, Workday appends that name with a number from 1 to 1000. If the first rule contains no information to create a username, Workday generates a 10-character, random username in its place.

Example: A user's name is John Smith, but there's another user with the same name. Since your first rule is a concatenation of a user's first and last name, Workday evaluates the next rule for information to create a unique username. After evaluating all rules and unsuccessfully generating a unique username, Workday returns to the first rule and creates johnsmith1, appending a number to make it unique.

Note: Workday doesn't use these rules to construct usernames when:

- A user's name is entered in non-Western script.
- A rule in a rule group doesn't produce a username. Example: You've configured a rule to use the user's employee number as a username component, and a user isn't an employee.

Workday will autogenerate a random 10-character alphanumeric username instead. You can use the **Edit Workday Account** task to change these usernames after Workday autogenerates them.

Steps

1. Access the **Maintain User Name Rules** task.
2. Add rows to a **Rule Group** to select the components from which to construct the username.
3. Rearrange the **Rule Order** in the order you want the components to display.
4. For each username component, select a **Substring Option** to specify the number of characters to use.
5. (Optional) Select the **Preserve Case Sensitivity** check box to preserve the case for letters in usernames generated automatically. You can't select this check box for numbers or special characters.

   Example: Use this check box to preserve case for first and last names so that Betty Liu's username is BLiu rather than bliu.
6. (Optional) Create additional rule groups to construct alternate usernames in case the previous rule group produces a duplicate.
7. To make new usernames more compatible with downstream applications and integrations that have username restrictions, consider:

Option	Description
Remove Special Characters and Spaces	Removes these ASCII special characters in usernames that Workday generates: !"#$%&'()* +,-./:;<=>?@[]^`{|}~´._. Doesn't modify the original username components, such as First Name or Last Name. You can manually construct usernames with special characters. You can't include the colon (:) or semicolon (;) in usernames. Workday removes them from automatically generated usernames regardless of the value for this setting. You also can't use the colon or semicolon in manually generated usernames.
Maximum User Name Length	Limits the number of characters for usernames generated automatically or manually. Workday automatically sets this value to zero, which indicates no limit, but you can set this value to

Option	Description
	10 or more. Any character in the Unicode Basic Multilingual Plane (BMP) counts as 1 character.

Edit Workday Accounts

Prerequisites

- Define user name and password requirements.
- Configure the *Edit Workday Account* business process and security policy in the System functional area.

Context

You can manage certain settings for specific Workday-managed accounts. Examples:

- Changing the account password of a user.
- Resetting the enrolled passwordless sign-in credentials for an account.
- Exempting a user account from multifactor authentication.
- Resetting the multifactor authentication configuration for a user.

Steps

1. Access the **Edit Workday Account** task.
2. As you complete the task, consider these general settings for the account:

Option	Description
Generate Random Password	Workday sends a random password to the **Email Address for Notifications** and requires a new password the next time the user signs in to Workday. You can't generate a random password if you've enabled delegated authentication for your tenant or for this account. To ensure that users receive security emails, you must select these check boxes on the **Edit Tenant Setup – Security** task: • **Email Temporary Password to New Accounts** • **Enable Security Emails** **Note:** The random password that Workday emails to users might contain special characters. Double-clicking such passwords won't select them in their entirety. Users should use some other method to select these passwords before copying them.
New Password **Verify New Password**	You can change passwords only for active accounts.
Do Not Allow UI Sessions	Select this check box to prevent integration system users from signing in to Workday through the UI. This option displays only for integration system users.

Option	Description
Account Disabled	Select this check box to terminate all active Workday sessions of the user on all devices immediately. For Payment Card Industry (PCI) users that Workday has locked out due to too many sign-in attempts, you can clear this check box to unlock their accounts. Workday doesn't update this field when you terminate an account.
Account Expiration Date	Set to terminate all active Workday sessions of the user on all devices at a specific date and time. If blank, the account doesn't expire. Workday automatically updates this field when you terminate an account.
Session Timeout Minutes	This value overrides the session timeout for the tenant set on the **Maintain Password Rules** task. When determining session age, Workday considers server requests that might take extra time, such as report results. For users that process credit card transactions, this value overrides the session timeout set on the **Maintain Payment Card Industry Password Rules** task.
Account Enabled for Data Masking	Workday masks fields containing sensitive data in all output this user generates.
Allow Mixed-Language Transactions	We recommend that you select this check box only for administrators who maintain translations. Workday displays transactions in English if they aren't available in the preferred language of the user. The result can be multiple languages displaying on the same page.
Display XML Icon on Reports	This option enables users to access reports through a REST API. Users must sign out and then sign in again to see the XML icon.
Reset Challenge Questions (Do Not Use)	Requires the user to configure challenge questions and answers the next time they sign in to Workday. **Note:** Workday plans to retire challenge questions in a future release.

3. Consider the **Reset Credentials** setting under **WebAuthn (FIDO2)** for the user account.

   Select the check box to reset all WebAuthn credentials that the account has enrolled for passwordless sign-in.

4. Consider these **Multi-factor Authentication** settings for the account:

Option	Description
Exempt Account	Exempts the user account from multifactor authentication.
Grace Period Enabled	Select to reset the number of times the user can sign in to Workday without enrolling in multifactor authentication. Clear to force the user to set up multifactor authentication the next time they sign in. Workday recommends that you reset the grace period if a user changes their mobile phone carrier or number.
Reset	Resets the multifactor authentication configuration shown in the **Type** column for the user, necessitating that they set it up again.

5. Consider these OpenID Connect settings for the account:

Option	Description
OpenID Identifier	The OpenID email address of the user. The incoming OpenID email address can't match the **Email Address for Notifications**.
OpenID Internal Identifier	Concatenation of the Workday environment and the OpenID GUID.
OpenID Connect Internal Identifier	Automatically populated *sub* value that the OpenID Connect provider passes to Workday.

6. Consider **Delegated Authentication Options** for the account:

   Note: Workday plans to retire delegated authentication in a future release. We recommend that you use other forms of authentication that we support.

Option	Description
Exempt From Delegated Authentication (Do Not Use)	You can enable 1 or more security administrator accounts to sign in to Workday with a Workday-managed authentication type, should your delegated system go offline.
Override Delegated Authentication Integration System (Do Not Use)	Changes the external identity management system that authenticates this account. Set the **Default Delegated Authentication System (Do Not Use)** on the **Edit Tenant Setup - Security** task.

7. Consider the notification settings for available notification types.

   Workday displays only the notification types that have routing rules containing allowed frequencies. You create and select notification routing rules for notification types in the **Notification Delivery Settings** section of the **Edit Tenant Setup - Notifications** task.

Related Information
Tasks
Enable or Disable Data Masking on page 275
Define Username Requirements on page 244
Define Password Rules on page 251

Reference

Reference: Edit Tenant Setup - Security
Reference: Edit Tenant Setup - Notifications

Create Workday Accounts Automatically

Prerequisites

Define the user name and password requirements on the **Maintain User Name Rules** and **Maintain Password Rules** tasks.

Context

You can configure the *Create Workday Account* service step on business processes to create Workday accounts automatically when those business processes run.

These steps only apply to Workday accounts, which are accounts that Workday manages.

Steps

1. Edit the business process that will contain the *Create Workday Account* service step.
2. If the business process already has a *Create Workday Account* step, ensure that the **Type** is *Service*.

   If your business process includes a *Reset Workday Account* service step, ensure that *Create Workday Account* occurs as a separate step after it, rather than as a shared step. Example: If your business process contains a *Reset Workday Account* step with an **Order** of b, add the *Create Workday Account* step so it has an **Order** of b1 or c.
3. In the *Create Workday Account* service step, click **Configure Create Workday Account**.
4. As you complete the **Create Workday Account Service Configuration** section, consider:

Option	Description
Email Destination	Sets the preferred destination for the new account email. Use the **Maintain Email Templates** task to configure the email that Workday sends. To ensure that users receive security emails, select the **Email Temporary Password to New Accounts** and **Enable Security Emails** check boxes on the **Edit Tenant Setup – Security** task.
Allow Mixed-Language Transactions	Enables users to access tasks that Workday hasn't translated into their preferred language. Workday displays untranslated fields in English, which can result in multiple languages displaying on the same page. Use the **Edit Tenant Setup - Global** task to enable languages for your tenant.

5. (Optional) Add a step after the *Create Workday Account* step to edit the account:
   a) Select *Action* as the **Type**.
   b) Select *Edit Workday Account* in the **Specify** field.
   c) Select the **Optional** check box.
   d) Select the **Group** to perform the step and the **Due Date**.

   You can't rescind this action; use the **Edit Workday Account** task to make changes.

Reset Workday Accounts for Terminated or Rehired Workers

Prerequisites

Security: *Set Up: Tenant Setup - Security* domain in the System functional area.

Context

You can use the *Reset Workday Account* event service on business processes to:

- Enable terminated employees to sign in to the Workday tenant to access items like tax documents.
- Restore the Workday accounts of terminated employees you rehire.

These steps only apply to Workday accounts, which are accounts that Workday manages.

Steps

1. Access the **Edit Tenant Setup – Security** task.
2. Select the **Email Temporary Password to New Accounts** and **Enable Security Emails** check boxes.
3. Access 1 of these business processes:
   - *Contract Contingent Worker*
   - *End Contingent Worker Contract*
   - *Hire*
   - *Termination*
4. Edit the definition for the business process and select an **Effective Date** for the business process change.
5. Add a step of **Type** *Service*.
6. From the **Specify** prompt, select **Reset Workday Account**.

   The *Reset Workday Account* event service resets an account but doesn't send username and password notification emails unless you configure it to do so.
7. (Optional) Set Up Notification Emails.
   a) Click **Configure Reset Workday Account**.
   b) Select the **Effective Date** of the event service change.
   c) Select **Generate One Time Use Password and email new account information**.
   d) Select an **Email Destination**.

      Example: In a hire business process, if **Email Destination** is set to **Send to work email. If no work email is available, send to home email**, and:

      - You are rehiring a former employee.
      - That former employee has a work email address in Workday.

      Workday sends a password reset email to the employee's work email address if that employee clicks the **Forgot Password?** link on the Workday sign-in page.

   If your business process includes a *Create Workday Account* service step, add the *Reset Workday Account* step as a separate step before it, rather than as a shared step. Example: If your business process contains a *Create Workday Account* step with an **Order** of g:

   - Add the *Reset Workday Account* step with an **Order** of g.
   - Change the **Order** of the *Create Workday Account* step to g1.

Result

Workday sends a sign-in link to terminated workers so terminated workers can sign in using their Workday-managed sign-in credentials.

When you rehire terminated workers, Workday removes the account expiration dates and enables the accounts of the workers. Former employees can access items secured by the Terminee as Self security group.

Note: If you rescind the hire, Workday again disables the Workday account, but the **Account Expiration Date** isn't set.

Next Steps

Add rehired workers to the user-based security groups they used to belong to.

Related Information

Tasks

Terminate User Accounts Automatically on page 255

Define Password Rules

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

You can configure tenant-wide password rules for accounts that Workday manages. Users must comply with these rules when they change or reset their Workday password. These rules apply only to permanent passwords, not temporary passwords. Workday maintains 2 different sets of password rules:

- A set that applies to users who process Payment Card Industry (PCI) information. You configure those rules on the **Maintain Payment Card Industry Password Rules** task. These users must belong to a security group secured to the *Manage: Credit Card Data* security domain.
- A set that applies to all other users in your tenant. You configure those rules on the **Maintain Password Rules** task.

Changes to password rules take effect immediately.

Steps

1. Access the **Maintain Password Rules** task or the **Maintain Payment Card Industry Password Rules** task.
2. As you complete the task, consider:

Option	Description
Maximum Inactive Days Before Disabling Account	(**Maintain Payment Card Industry Password Rules** task only) This value must be 90 or fewer.
Minimum Password Length	Workday account passwords must contain at least 8 characters. PCI passwords must contain at least 7 characters.
Maximum Password Age in Days	For PCI passwords, this value must be 90 or fewer.
Number of Passwords Before Password Reuse	For PCI passwords, this value must be at least 4.
Failed Signon Attempts Before Lockout	The number of consecutive times users can perform these actions from an untrusted device before Workday locks them out:

Option	Description
	• Enter an incorrect password when signing in to Workday. • Answer challenge questions incorrectly. If a user reaches the maximum attempt value, Workday locks the account on the next unsuccessful attempt. Example: When set to 5, if you enter the password incorrectly 3 times and answer challenge questions incorrectly 3 times, Workday locks you out. If the third attempt to answer the challenge question is successful, Workday doesn't lock the account, and we reset the counter. Should Workday lock an account from an untrusted device, the account owner has 20 additional attempts to sign into the account and unlock it from a device they've trusted. Once the user reaches the 20-attempt threshold from a trusted device, Workday locks the account and removes the trust relationship for the device. For PCI password configuration, Workday locks the account for at least 30 minutes. For **Lockout Until Enabled by Administrator**, Workday locks the account until you unlock it on the **Edit Workday Account** task.
Number of Failed Password Reset Attempts Allowed	(**Maintain Password Rules** task only) The number of consecutive times (between 1 and 5, inclusive) a user can perform these actions before they must contact an administrator: • Click the **Forgot Password** link. • Fail to reset their password. If they reach this limit, they can still sign in if they enter the correct password. Workday automatically sets this value to 3. This setting doesn't apply if an administrator has locked the account. You can use the **Edit Workday Account** or **Manage Workday Account Credentials** task to verify if a user has reached this limit (**Maximum Forgot Password Requests** check box).
Force Password Reset Upon Login	Workday requires PCI users to change their password the next time they sign in to Workday if their password doesn't meet updated password rules.
Session Timeout	Limits the amount of time an account can be idle. If a PCI user session is idle for more than 15 minutes, the user must reenter their password to sign in to Workday. For other users, specify a value less than 720 minutes to apply to:

Option	Description
	• Users for whom you haven't specified a **Session Timeout Minutes** value on the **Edit Workday Account** task. • All users in the tenant.
System Users exempt from password expiration	Passwords for non-PCI users entered here don't expire. You can't exempt PCI users from password expiration. You can't remove certain Workday-owned accounts, such as wd-support and wd-environments, because they're automatically exempt from password expiration.

Next Steps

Access these reports to verify your password rules:

- **Password Rules Configuration**
- **Payment Card Industry Password Rules Configuration**

Related Information
Tasks
Edit Workday Accounts on page 246

Configure Password Reset

Prerequisites

Security: These domains in the System functional area:

- *Set Up: Tenant Setup - Security*
- *Set Up: Tenant Setup - BP and Notifications*

Context

You can configure how users can reset and change their passwords for Workday accounts. Workday accounts are accounts that Workday manages.

Note: For information on how to configure password reset for accounts that Workday doesn't manage, contact the manager of those accounts. Example: Your delegated authentication or third-party identity provider.

Workday can recover forgotten passwords for Implementer accounts if the Workday account has the required contact information.

Workday rejects password reset for a user when:

- The account is currently expired or disabled.
- The information the user enters doesn't match the information stored in Workday. If the user name is valid, Workday sends an email to the primary email address of the user, if provided. The email notifies the user of the failed reset attempt.

Steps

1. Access the **Edit Tenant Setup - Security** task.

2. Select the **Enable Security Emails** check box to enable Workday to send security-related email notifications to users, and select 1 of the preferred email destination options.

   Example: If you want users to receive password reset email notifications at their home email address only if they don't have a work email address set up on their Workday account profiles, select the **Send to work email, else home email** email destination option.
3. Select the **Enable Forgotten Password Reset** check box and select 1 of these password reset options:

Option	Description
Reset Password Online	Requires a user to answer 3 challenge questions before Workday directs them to a password reset page. Workday sends a confirmation email when: • The user has a valid email address stored in Workday. • You select **Enable Security Emails**.
One Time Use Link	Requires a user to enter their user name and a primary email address for their account before Workday sends them a link to a password reset page. The link expires after the user clicks it or after 1 hour, whichever occurs first. An account can't have more than 5 valid links at any time. The email address that they enter must exist as a primary email address in their Workday profile and be compatible with the preferred email destination option you selected on the **Edit Tenant Setup - Security** task. Example: If you selected the **Send to work email only** destination option, they must enter their user name and primary email address that exists in the **Work Contact Information** portion of their Workday profile. If they enter their home email address, they won't receive the password reset email.

4. To ensure that the **Change Password** link displays on the Workday sign-in page, select the **Enable Change Password Link** check box.
5. (Optional) In the **Custom Password Reset Error Message** field, specify an error message that displays when users answer security questions incorrectly. Before the error message can display:
   a. Clear the **Enable Change Password Link** check box.
   b. Set up tenant-wide challenge questions.
6. Access the **Edit Tenant Setup - Notifications** task and verify that there are no email channel restrictions set up in the **General Notification Restrictions** grid for your tenant environment.

Result

Users can:

- Change their Workday password by:
  - Clicking the **Change Password** link on the Workday sign-in page.
  - Selecting **Change My Password** for their Workday account.
- Reset their Workday password by clicking the **Forgot Password** link on the Workday sign-in page.

Next Steps

Review the **Signons and Attempted Signons** report.

Related Information

Concepts

Concept: Configurable Security on page 112

Tasks

Edit Workday Accounts on page 246
Manage Challenge Questions on page 32
Require Challenge Questions at Sign-In on page 32
Steps: Set Up Contact Information

Reference

Reference: Edit Tenant Setup - Security
Reference: Edit Tenant Setup - Notifications

Terminate User Accounts Automatically

Prerequisites

Security: These domains in the System functional area:

- *Business Process Administration*
- *Manage: Business Process Definitions*

Context

You can disable the accounts of terminated workers or nonworkers (such as Academic Affiliates) automatically, by changing the definition of these business processes:

- *End Academic Appointment*
- *End Contingent Worker Contract*
- *Termination*

These steps only apply to Workday accounts, which are accounts that Workday manages.

Steps

1. Edit the business process definition.
2. Add a new step to remove the worker or nonworker from user-based security groups.
   a) Assign the order number for the step in the business process.
   b) Under **Type**, select *Service*.
   c) Under **Specify**, select *Remove User-Based Security Groups*.
   d) Select the **Due Date Is Based On Effective Date** check box.
   e) Click **OK**.
   f) (Optional) From the related actions menu of the step, select **Business Process** > **Maintain Step Delay**.
      1. Select the **Effective Date**, and then click **OK**.
      2. In the **Delay Is Based On** section, select **Field**, and then select **Effective Date** from the prompt.

3. Add another step to disable the Workday account of the worker or nonworker.
   a) Assign the order number for the step in your process to be the next step after the *Remove User-Based Security Groups* service.
   b) Under **Type**, select *Service*.
   c) Under **Specify**, select the *Terminate User Account* service from the prompt.
   d) Select the **Due Date Is Based On Effective Date** check box.
   e) Click **OK**.
   f) Click the **Configure Terminate User Account** button.
   g) Specify the **Effective Date**, and click **OK** to display hidden options. When you don't specify an effective date, Workday deactivates the account at midnight on the day of termination. Example: You terminate a worker on April 7. Workday deactivates their account on April 7 at midnight if you don't specify an effective date.
   h) Select either the *Use Termination Date* or *Use Last Date Worked* of the user as the expiration date of their user account.
   i) Select the **Account Termination Time** from the list.

Result

When the user account expires:

- Workday terminates all active Workday sessions from all devices (such as desktop browsers, Workday on iPhone, and Workday on iPad).
- The user is unable to sign in.

The termination date and time are based on:

- The local time of the location of the user, if specified;
- Otherwise, the tenant **Default Timezone**, if specified;
- Otherwise, the server time (typically Pacific time).

If you rescind the business process:

- Workday clears the user account expiration date.
- You must manually restore the membership of the user in user-based security groups.

Because terminated accounts remain in Workday with an expiration date that is in the past, you can't reuse the user account ID.

Authorized users can still manually edit the user account expiration date.

Related Information
Tasks
Edit Business Processes
Maintain Step Delay
Reset Workday Accounts for Terminated or Rehired Workers on page 250
Reference
Reference: Edit Tenant Setup - System

Terminate User Account Manually

Prerequisites

Security: *Business Process Administration* and *Manage: Business Process Definitions* domains in the System functional area.

Context

You can disable the accounts of workers or nonworkers manually, such as when business processes don't include a step to disable the accounts automatically. Examples:

- *Termination*
- *End Contingent Worker Contract*

These steps only apply to Workday accounts, which are accounts that Workday manages.

Steps

1. If the worker is a member of user-based security groups, remove those groups from the account of the worker.
   a) Select **Security Profile** > **Assign User-Based Groups** from the related actions menu of the worker.
   b) Delete all items in the **User-Based Groups to Assign** list.
2. Select **Security Profile** > **Edit Workday Account** from the related actions menu of the worker.
3. Disable the account:
   - To disable the account immediately, select the **Account Disabled** check box.
   - To disable the account later, enter a date and time in the **Account Expiration Date** field.

Result

When Workday disables the user account:

- Workday terminates all active Workday sessions from all devices, such as desktop browsers and mobile apps on iPhone or iPad.
- The user is unable to sign in.

The termination date and time are based on:

1. The local time of the location of the worker, if specified.
2. The tenant **Default Timezone**, if specified.
3. The server time (typically Pacific time).

Because terminated accounts remain in Workday with an expiration date that is in the past, you can't reuse the user account ID. Authorized users can still manually edit the expiration date of the user account.

Next Steps

You can add a notification to these business processes, to notify Security Partners that they must disable the account of terminated workers manually:

- *Termination*
- *End Contingent Worker Contract*

Related Information
Tasks
Edit Business Processes
Maintain Step Delay
Reset Workday Accounts for Terminated or Rehired Workers on page 250
Reference
Reference: Edit Tenant Setup - System

Lock and Unlock Workday Accounts

Prerequisites

Security: *Lock Out Workday Accounts* domain in the System functional area.

Context

You can lock Workday accounts to prevent specific users from signing in to Workday and updating data. You can also restore access for users that you've locked out. You can't restore access for users that Workday has locked out due to excessive failed sign-in attempts.

Workday automatically prevents you from locking or unlocking your own account or any account you don't have access to.

These steps only apply to Workday accounts, which are accounts that Workday manages.

Steps

1. Access the **Manage Workday Accounts** task.
2. As you complete this task, consider:

Option	Description
Select All	Locks or unlocks all Workday accounts.
Include Selected Workday Accounts	Locks or unlocks the Workday accounts that you specify.
Exclude Selected Workday Accounts	Locks or unlocks all Workday accounts except for the accounts that you specify. If you enable external sites for your tenant, such as Workday Recruiting or Student, Workday adds the Workday user for those sites to this exclusion list. If you remove a Workday user from the list, you lock the site; Workday doesn't automatically add the user to the list again. To ensure scheduled operations complete, select the Workday accounts for owners of all jobs, integrations, and reports to exclude from the restriction.

Result

Users can't access Workday when you've locked their accounts. Workday sends an email to users with locked accounts when they try to sign in.

Next Steps

You can use these reports to display locked user accounts:

- **All Workday Accounts**
- **Workday Accounts Currently Locked Out By Excessive Failed Signon Attempts**

These reports are secured to the *Workday Accounts* domain in the System functional area.

End Active Sessions for Multiple Workday Accounts

Prerequisites

Security: *Security Administration* domain in the System functional area.

Context

When performing a bulk data load or other Workday maintenance, you can use the **Manage Workday Maintenance Window** task to end active sessions, including integrations and other background processes. This session ending ensures that no unwanted updates to data can occur. Workday doesn't automatically restart terminated processes. Session restrictions automatically exclude the user who creates the restriction.

Users can access self-service tasks, including **End All Active Sessions**, to end their own UI sessions. These tasks don't end active sessions for other user accounts.

You can use the **Manage Workday Accounts** task to prevent all access to Workday.

Steps

1. Access the **Manage Workday Maintenance Window** task.
2. As you complete the task, consider:

Option	Description
Restrict New Sessions	Locks the tenant and prevents users from creating new sessions.
Allow New Sessions	Unlocks the tenant and enables users to create new sessions. This option is only available following a **Restrict New Sessions** or **Restrict New Sessions and End Existing Sessions** action.
Restrict New Sessions and End Existing Sessions	Locks the tenant, ends active sessions, and prevents users from creating new sessions.
System Accounts Excluded from Session Restriction	If you enable Workday Recruiting, Student, or other external sites for your tenant, Workday automatically adds the Workday account for those sites to this exclusion list. To ensure scheduled operations complete, select the Workday accounts for owners of all jobs, integrations, and reports to exclude from the restriction. If a scheduled integration uses an excluded account for *Run As User*, then that integration still runs. Workday recommends creating an integration system user (ISU) account for scheduled integrations to ensure that: • Users needing to perform work during the tenant lock out period can continue to do so without suspending the integrations.

Option	Description
	• Workday authenticates the ISU and the integration completes, even if the user who scheduled the integration leaves the company.

Next Steps

Access the **Manage Workday Maintenance Window** task and select **Allow New Sessions** to enable users to create new sessions.

External Accounts

Manage External Accounts

Prerequisites

Security:

- *Manage: Candidate Account* domain in the Recruiting functional area.
- *Manage: Student External Site Account* domain in the Academic Foundation functional area.
- *Manage: Supplier External Site Account* domain in the Supplier Accounts functional area.

Context

Workday enables you to manage external accounts to:

- Prevent users from signing in to Workday-managed external web sites, or restore access for users previously locked out of the site. You can't restore access for external users that Workday locks out due to excessive failed authentication attempts. Workday automatically unlocks such accounts after 30 minutes.
- Enforce a password reset for specific external user accounts or all external user accounts. You can only enforce a password reset when the passwords for the accounts were last reset before a specified effective moment.
- Configure password rules for candidates, students, or suppliers separate from the rules for internal users.

Steps

1. Access the **Manage External Accounts** task.
2. As you complete the task, consider:

Tab	Description
Lock Accounts	When you select the **Include Selected External Accounts** option to lock specific accounts, Workday unlocks all other accounts of the type selected when you run the task.
Reset Passwords	Configure a past time and date in the **Effective Moment** field. Check the **Exclude New Accounts** check box to exempt accounts created after the **Effective Moment** from password resets. Workday uses this configuration to determine when to enforce password resets for selected external accounts.

Tab	Description
Password Rules	Workday enables you to set a: • Minimum password length between 8 and 99 characters. • Maximum password length between 64 and 128 characters. If you don't want to impose a maximum password length limit, you can specify a maximum password length of zero. Changes to password rules take effect immediately, but Workday doesn’t force users to change their passwords. When a user changes their password, they must comply with the latest password rules.

Concept: User Accounts for External Sites

Workday supports external site accounts for:

- Candidates. Candidates can create accounts on external sites. This includes candidates who apply using an external career site, are submitted through a recruiting agency, or had a job application created using the **Create Job Application** task. You can't create candidate accounts using web services.
- Prospective suppliers. Prospective suppliers can create accounts on external supplier sites to submit information to your company for review and approval. You can't create supplier accounts using web services.
- Student prospects. Student prospects can create accounts on external student sites to apply for admission. Workday also creates accounts when you use the *Import Student Applications* web service or the **Create Account** task.

Update External Account Email

You can use the **Update External Account Profile** task (secured to the *Manage: Candidate Account* domain in the Recruiting functional area) to update an external account email for a user, which is also their username.

When you complete this task, Workday sends a notification email to the old email address and a verification email to the new email address. If you don't trust the old email address, you can elect not to send an email to the recipient.

Workday updates the username after the user clicks the verification link from their new email address and enters their password. Users who forget their password can't complete this process.

Account Verification for Candidates

For external career sites, you can determine the account setup steps for candidates using your home account and verification email settings on the **Edit Tenant Setup – Recruiting** task. If you don't select the account or verification email option, candidates can apply without creating an account.

Related Information
Reference
Reference: Edit Tenant Setup - Recruiting

Reference: Track Sign-In Activity for External Sites

Workday provides reports to track sign-in activity for your external sites.

Signons and Attempted Signons Reports

Use these reports to review details about sign-in attempts for valid accounts:

- **Candidate Signons and Attempted Signons**
- **Student Signons and Attempted Signons**
- **External Supplier Signons and Attempted Signons**

Invalid User Signon Attempts Reports

Use these reports to review details about sign-in attempts for unidentified accounts:

- **Candidate Invalid User Signon Attempts**
- **Student Invalid User Signon Attempts**
- **Supplier Invalid User Signon Attempts**

Note: These reports might display candidate IP addresses for tenant sign-ins, depending on sign-in date and tenant environment:

- **Candidate Signons and Attempted Signons**
- **Candidate Invalid User Signon Attempts**

Use caution when sharing these reports, and don't share them outside of your organization.

When reviewing these reports, consider:

Field	Description
Attempted At	Displays the Workday server time.
Invalid User Name	Provides more detailed information about the sign-in attempt.
Authentication Failure Message	Provides details about a failed sign-in attempt.

User Provisioning Workspace

Steps: Set Up User Provisioning Workspace

Prerequisites

Security:

- *Set Up: User Provisioning* domain in the System functional area.
- *Manage: Workday Strategic Sourcing User Provisioning* domain in the System functional area.
- *Report: User Provisioning Status* domain in the System functional area.

Context

The User Provisioning Workspace (UPW) enables you to authenticate and sync users to the Workday suite of products.

Workday recommends using roles like security administrator to set up the UPW, while account managers can configure products and view error reports.

Steps

1. Access the User Provisioning Workspace.
   See Set Up Access to User Provisioning.

2. Create provisioning groups, populate them with security groups, and associate those provisioning groups with a product in the Workspace.

   See Create User Provisioning Groups.
3. Generate a Preview Report.

   See Create Preview Reports.
4. To sync users, select **Preview and Enable Sync** from the **Configuration** page of a Workday product. Click both the check box and **Enable Sync** options to proceed with synchronization.

Next Steps

Verify that users can access products with their Workday credentials.

Related Information

Examples

2024R1 What's New Post: User Provisioning Workspace

Set Up Access to User Provisioning

Prerequisites

Security:

- *Set Up: User Provisioning* domain in the System functional area.
- *Manage: Workday Strategic Sourcing User Provisioning* domain in the System functional area.
- *Report: User Provisioning Status* domain in the System functional area.

Context

To access the User Provisioning Workspace, you first have to configure it in Workday. The configuration process is comprised of enabling security groups for provisioning and setting up access to the Workspace.

Steps

1. Access the **Maintain Dashboards** report.
2. Edit the **Home** dashboard.
3. Add the **Manage User Provisioning for Workday Products** worklet to the **Worklets** table.
4. In the **Required for Groups** column, add security groups you'd like to access the worklet.
5. Select the **Required?** check box to prevent users from removing the worklet from their Home page.
6. From the Home page, access the **Manage User Provisioning for Workday Products** worklet.
7. From the **Manage User Provisioning for Workday Products** worklet page, select **Set Up Security Groups for User Provisioning**. Add one or more groups to the **Security Group** grid.

   Note: Enabling security groups for provisioning doesn't automatically provision those groups for a Workday product. Instead, the User Provisioning Workspace enables you to provision users.

Next Steps

Once you configure access to the User Provisioning Workspace, you can create provisioning groups.

Related Information

Concepts

Concept: User Provisioning on page 267

Examples

2024R1 What's New Post: User Provisioning Workspace

Create User Provisioning Groups

Prerequisites

Security:

- *Set Up: User Provisioning* domain in the System functional area.
- *Manage: Workday Strategic Sourcing User Provisioning* domain in the System functional area.
- *Report: User Provisioning Status* domain in the System functional area.

Context

To provide users access to the Workday suite of products, you must create provisioning groups in the User Provisioning Workspace (UPW). The provisioning process doesn't authorize users to carry out tasks or actions in Workday products.

Steps

1. In Workday, select the **Manage User Provisioning for Workday Products** worklet.
2. From the **User Provisioning Workspace Links** section, click *User Provisioning Workspace*.
3. From the **Products** section of the Workspace landing page, click **Configure** on the product you want to create provisioning groups for.
4. Using the **Workday Security Groups** drop-down, add one or more security groups to the provisioning group. Only security groups that you enabled for user provisioning in the **Manage User Provisioning for Workday Products** worklet are available in the drop-down.
5. Once you click **Create Provisioning Group**, you can add or remove security groups by selecting **Edit Provisioning Group** from the **Configuration** tab of a product.

   Note: Changing the security groups that make up a provisioning group, or the connection between an active provisioned group and a Workday product will prompt the reevaluation and potential deprovisioning of users.
6. To view other configuration changes made to a provisioning group by members of your organization, access the *Configuration Logs* section of a product's **Configuration** tab.

Next Steps

Once you create and link a provisioning group to a Workday product, you can generate a preview report.

Related Information
Concepts
Concept: User Provisioning on page 267
Examples
2024R1 What's New Post: User Provisioning Workspace

Create Preview Reports

Prerequisites

Security:

- *Set Up: User Provisioning* domain in the System functional area.
- *Manage: Workday Strategic Sourcing User Provisioning* domain in the System functional area.
- *Report: User Provisioning Status* domain in the System functional area.

Context

Preview reports enable you to identify any issues that might occur in the provisioning process, including users who might not have accounts in both Workday and a Workday-owned product.

Steps

1. Once you've created provisioning groups, access the **Preview Report** in the **Configuration** tab of a provisioning group.
2. Click **Preview and Enable Sync**.

   It can take time for the report to generate. You can safely exit out of the User Provisioning Workspace and check back later for the results of the report.
3. Verify how many **New Users** need accounts in the target application.
4. Users in **Users Not in Provisioning Group** have accounts in the target application but aren't in the security groups that make up a provisioning group. To resolve this issue, enable additional security groups in the **Manage User Provisioning for Workday Products** worklet.
5. **Invalid Users** can't sync due to email-specific errors. These errors occur when a user doesn't have a unique email in Workday or 2 users have the same email. Contact individual users who have mismatched or duplicate information, and confirm their account emails before enabling sync.
6. You can also access the **Users** section of a Workday product page to confirm users' provisioning information.

Next Steps

Select both the check box and **Enable Sync** button located on the **Configuration** tab to synchronize the provisioning group across Workday and the Workday-owned product. The **Sync** label will change from *Off* to *On* once synchronization is complete. You can also access the **Sync Report** tab to assess any provisioning or deprovisioning errors during synchronization.

Related Information
Concepts
Concept: User Provisioning on page 267
Examples
2024R1 What's New Post: User Provisioning Workspace

Example Steps: Deprovision Terminated Workers

This example illustrates how to deprovision terminated workers.

Context

You want to ensure that a terminated worker is automatically deprovisioned from accessing Workday Strategic Sourcing (WSS). To comply with state and federal regulations, however, you also need to maintain the worker's account for the duration of severance payments. After resetting and temporarily enabling the terminated worker's account, you use the error and preview reporting features in the User Provisioning Workspace (UPW) to confirm their deprovisioning.

Prerequisites

Security: These domains in the System functional area:

- *Manage: Workday Strategic Sourcing User Provisioning*
- *Report: User Provisioning Status*
- *Tenant Setup - Security*
- *Set Up: User Provisioning*

Steps

1. Reset the terminated worker's account to enable them temporary access and set an **Account Expiration Date**.

   See: Reset Workday Accounts for Terminated or Rehired Workers.
2. Access the **Edit Workday Account** task. Clear the **Account Disabled** check box for the terminated worker.

   See: Edit Workday Accounts.
3. Access the **View Security Groups for User** report to confirm that the terminated worker is a member of the **Terminee as Self** Workday-delivered security group.

   See: Concept: Configurable Security.
4. Access the User Provisioning Workspace. Ensure that the worker you want to deprovision is no longer a member of security groups enabled for use in the UPW.

   See: Set Up Access to User Provisioning.
5. In the **Users** section of the User Provisioning Workspace, search for the terminated worker. Access the *Activity Log* to verify that they're deprovisioned.
6. In the **Provisioning Status** tab of the WSS application page, confirm that deprovisioning is complete. If deprovisioning has failed, or completed with errors, check the User Details report to identify error messages and the date of occurrence.

   See: Create Preview Reports.

Example Steps: Provision Workers Returning from Leave

This example illustrates how to provision workers who were deprovisioned while on medical leave.

Context

A worker recently went on medical leave, which resulted in the deprovisioning of their account, preventing them from accessing Workday Strategic Sourcing (WSS). After reactivating the worker's account, you use the error and preview reporting features in the User Provisioning Workspace (UPW) to confirm that the worker is provisioned again.

Prerequisites

Security: Configure these domains in the System functional area:

- *Manage: Workday Strategic Sourcing User Provisioning*
- *Report: User Provisioning Status*
- *Set Up: User Provisioning*

Configure this business process in the System functional area:

- *Edit Workday Account*

Steps

1. Access the **Edit Leave Type** task.
   a) From the **Leave Type** prompt, select **Medical Leave>Illness or Injury**.
   b) Under **Leave Impacts**, clear the **Inactivate ~Worker~** check box.
   c) Click **OK** and **Done**.

   See: Create Leave Types.
2. Review the worker's *Return from Leave of Absence* request.

   See: Concept: Leave of Absence Business Processes.
3. Access the **Edit Workday Account** task. Clear the **Account Disabled** check box.

   See: Edit Workday Accounts.

4. Access the User Provisioning Workspace. Ensure that the returning worker is a member of security groups enabled for use in the UPW.

   See Set Up Access to User Provisioning.
5. In the **Users** section of the UPW, search for the returning worker. Access the *Activity Log* to verify that the user is provisioned.
6. In the **Provisioning Status** tab of the WSS product page, confirm that provisioning is complete. If provisioning has failed, or completed with errors, check the User Details report to identify error messages and the date of occurrence.

   See Create Preview Reports.

Concept: User Provisioning

User Provisioning is a unified method for enabling users access to the Workday suite of products. Using a centralized User Provisioning Workspace (UPW), customers can provision accounts, sync user data, and authenticate users. The workspace also automates the evaluation and deprovisioning of former user accounts.

User provisioning consists of:

Term	Definition
Preview Report	Located in the UPW, preview reports identify account matching and synching discrepancies between Workday and target products. Users in the report will have 1 of 4 statuses: • *Matched*, which indicates that a user has an account in both the provisioning group and the target Workday product. • *New*, which indicates that a user will get an account in the target Workday product. • *Not in Provisioning Group*, which indicates that a worker has an account in the target product but not in the provisioning group. • *Invalid*, which is an error that will occur during provisioning. One type of invalid error is *Invalid resource: Username is required*. This error can be resolved by ensuring that users have a unique work email in Workday. Another invalid error indicates that two users have the same email address.
Provisioning Group	Made up of one or more security groups, provisioning groups determine which users can access applications. Creating provisioning groups doesn't authorize users to perform actions in Workday products.
User Provisioning Workspace	The Workspace enables administrators to provision user access to Workday products.
User Synchronization	Enabling user synchronization transfers provisioned user data to Workday products.

Related Information
Tasks
Set Up Access to User Provisioning on page 263

Create User Provisioning Groups on page 264
Create Preview Reports on page 264

Examples

2024R1 What's New Post: User Provisioning Workspace

Unified Access Management

Steps: Set Up Unified Access Management (UAM)

Prerequisites

Before enabling UAM, complete Set Up SAML SSO into Adaptive Planning for Synced Users.

To request this feature, contact your Named Support Contact to submit a Workday Customer Care request. After confirming that you're eligible, we'll enable the feature.

Configure these domains in the System functional area:

- *Unified Security Administration*
- *Set Up: Adaptive Planning Group Sync*

Adaptive Planning admin permissions:

- *Admin Access > Users*
- *Admin Access > Permissions*

Note: If you want to enable UAM for a non-Production environment, use a Workday IMPL tenant rather than Sandbox. Due to the weekly tenant refresh, Sandbox tenants are wiped of any changes you make to UAM policies. This results in a nonfunctional tenant.

Context

Unified Access Management enables you to automate the management of permissions and security groups across Workday and Adaptive Planning. By migrating, configuring, and syncing permission sets with their equivalent action groups in Workday, you can ensure that changes to permissions update automatically.

Steps

1. Access the **Migrate Adaptive Planning Permission Sets and Assignments** task to copy permission sets and user assignments from Adaptive Planning.

   Note: As you migrate information from Adaptive Planning, you can access the **User Permissions Comparison Report** in Workday to identify information that didn't sync.

   See Migrate Permission Sets and User Assignments from Adaptive Planning on page 269.
2. Access the **Create Action Group** task to configure action groups that didn't migrate from Adaptive Planning.

   See Create Action Groups.
3. Access the **Create Authorization Policy** task to link new action groups to user groups. Authorization policies ensure that changes in users or actions sync between Workday and Adaptive Planning.

   As you create or update action groups, authorization policies, or user groups in Workday, check the **View Action Group Details** report to confirm that information is consistent between Workday and Adaptive Planning.

   See Create Authorization Policies on page 271.

4. Access the **Maintain UAM User Integration** task to add ISU users to UAM.

   See Set Up Unified Access Management (UAM) User Integration on page 271.
5. Access the **Activate UAM Integration with Adaptive Planning** task to enable UAM for your Planning instance.
6. Access the **Subscribe User Groups for Adaptive Planning** task to specify security groups to sync with Adaptive Planning.

   See Sync User Groups with Adaptive Planning on page 272.
7. Access the **Notify Authorization Policy Changes to Adaptive Planning** report to sync permission changes in real time.

Related Information
Examples
Feature Release Note: Unified Access Management (UAM)

Migrate Permission Sets and User Assignments from Adaptive Planning

Prerequisites

Security:

- Workday HCM: *Unified Security Administration* domain in the System functional area.
- Adaptive Planning: *Admin Access* permission and users.

Context

UAM enables you to migrate permission sets and user assignments from Workday Adaptive Planning to Workday HCM. During the migration process, you can use comparison reports in Workday to determine what permission sets have equivalent action groups. After you migrate permission sets, you can use reports to confirm, and adjust, information that didn't sync.

Steps

1. Enable the *Unified Security Administration* domain in the System functional area.

   See Steps: Enable Functional Areas and Security Policies.
2. Access the **User Permissions Comparison Report** to check that user permissions match between Workday and Adaptive Planning.
3. Access the **Migrate Adaptive Planning Permission Sets and Assignments** task to copy permission sets and group assignments from Adaptive Planning.
4. You can also access the **Create Action Group** task to create groups for permission sets that failed to migrate from Adaptive Planning.
5. After migrating, rerun the **User Permissions Comparison Report** to confirm that permissions match for each user.
6. You can then access the **View Action Group Details** and **View User Group Details** reports, and adjust settings in both Workday and Adaptive Planning to address any discrepancies.

Next Steps

Once you've migrated permissions from Adaptive Planning and created any additional action groups, you then need to configure authorization policies and user groups. When you set up UAM and enable the **Activate UAM Integration with Adaptive Planning** task, both the **Migrate Adaptive Planning Permission Sets and Assignments** task and **User Permissions Comparison Report** will no longer be available.

Create Action Groups

Prerequisites

Security: *Unified Security Administration* domain in the System functional area.

Context

Also referred to as permission sets in Workday Adaptive Planning, action groups enable you to define which actions users can perform in Workday. Action groups are similar to domains, except that you manage the tasks contained in a group.

Steps

1. Access the **Create Action Group** task.
2. As you complete the task, consider:

Option	Description
Application Instance	Select an Adaptive Planning instance.
Name	Enter a name that describes the actions in this group.
Actions	Select one or more actions to group together. **Note:** When you select some variation on the same action, Workday automatically adds the parent action to the action group. Example: If you select *Access Sheets: Download to Excel*, Workday then selects the parent action *Access Sheets*.

3. To change an action group, access the **Edit Action Group** task.
4. You can regularly use the **View Action Group Details** report to filter and verify which actions, authorization policies, and users are associated with specific groups. This report also enables you to search for action groups related to a specific application and instance.
5. (Optional) When you make changes to action groups, authorization policies, or other related information, you can access the **Notify Authorization Policy Changes to Planning** task to immediately sync those changes with Adaptive Planning. Otherwise, Workday syncs with Adaptive Planning on an hourly basis.

   To access the notification task, enable these admin permissions in Adaptive Planning:

   - *Admin Access > General Setup*
   - *Admin Access > Users*

   If multiple Planning instances are linked in an instance tree, the notification task will require you to activate all instances in UAM.

Example

You want to create an Administrative action group in Adaptive Planning. You access the **Create Action Group** task and enter "Administrative Actions" as the name of the action group. In the **Actions** field, you select *Access Sheets*, *Access Dashboards*, *Access Reports*,*Access Transactions*, and any other actions (permissions) required for this role.

Next Steps

Before you create an authorization policy, you'll need to create or modify a user group. You can access the **View User Group Details** report to view existing user groups before creating additional groups.

Create Authorization Policies

Prerequisites

Security: *Unified Security Administration* domain in the System functional area.

Context

Authorization policies enable you to tie role-based, user-based, or integration system security groups to a series of actions listed in an action group. By linking user groups and action groups to an authorization policy, you enable users to carry out actions in Workday Adaptive Planning.

Steps

1. Access the **Create Authorization Policy** task.
2. As you complete the task, consider:

Option	Description
Application Instance	Select an Adaptive Planning instance.
Name	Enter.
Description	(Optional) Enter.
Action Groups	Enter one or more action groups that you want to assign to an authorization policy.
User Groups	Select any role-based, user-based, or integration system security group that you want to have access to Adaptive Planning.
Enabled	Check.

3. To edit an existing authorization policy, access the **Edit Authorization Policy** task.
4. (Optional) When you make changes to action groups, authorization policies, or other related information, you can access the **Notify Authorization Policy Changes to Adaptive Planning** task to immediately sync those changes with Adaptive Planning. Otherwise, Workday syncs with Adaptive Planning on an hourly basis.

   To access the notification task, enable these admin permissions in Adaptive Planning:

   - *Admin Access > General Setup*
   - *Admin Access > Users*

   If multiple Planning instances are linked in an instance tree, the notification task will require you to activate all instances in UAM.

Set Up Unified Access Management (UAM) User Integration

Prerequisites

Security: *Unified Security Administration* domain in the System functional area.

Context

While user groups automatically sync with UAM using Workday Power of One, integration system users (ISU) aren't included in those groups. The **Maintain UAM User Integration** task enables you to sync ISU users with UAM, before activating UAM integration with Adaptive Planning. We recommend accessing this task after creating an authorization policy. If you activate UAM integration before migrating permission sets and setting up authorization policies, comparison reports won't work.

Steps

1. Access the **Maintain UAM User Integration** task.
2. As you complete the task, consider:

Option	Description
Application	Adaptive Planning.
Application Instance	Select an Adaptive Planning instance.
User Groups	Select one or more user groups to sync with UAM. **Note:** If you delete the Adaptive Planning user group, Workday will add it back to the **User Groups** field once you click **OK**. This ensures that the baseline Adaptive Planning group can interact with the Adaptive Planning application.

Next Steps

Once you've migrated permission from Adaptive Planning, configured user groups, created authorization policies, and added ISU users to UAM, access the **Activate UAM Integration with Adaptive Planning** task to complete the setup process.

Sync User Groups with Adaptive Planning

Prerequisites

Security: *Set Up: Adaptive Planning Group Sync* domain in the Adaptive Planning functional area.

Context

The **Subscribe User Groups to Adaptive Planning** task enables you to sync Workday security groups with Adaptive Planning. Once synced, you can use these security groups to configure users' access to Adaptive Planning resources. Users who aren't members of an Adaptive Planning instance won't properly sync with UAM and Adaptive Planning.

Steps

1. Access the **Subscribe User Groups to Adaptive Planning** task.
2. Enter an Adaptive Planning **Application Instance**.
3. In the **User Groups** field, enter the role-based, user-based, or integration system security group that you want to sync with Adaptive Planning.
4. (Optional) When you make changes to security groups, you can access the **Sync User Groups** task to immediately sync those changes with Adaptive Planning. Otherwise, Workday will sync with Adaptive Planning on an hourly basis.

Concept: Unified Access Management (UAM)

In Workday Adaptive Planning, administrators must create and assign permission sets on a manual, user-by-user basis. To streamline these manual processes, you can use Unified Access Management (UAM) to create and maintain action groups (permission sets), security groups (user groups), and authorization policies (permission set assignments) in Workday. Any updates made to user and security group information in Workday then sync with Adaptive Planning to enable the continual management of user entitlements.

Action Groups

Action groups are the functional equivalents of permission sets in Adaptive Planning. Similar to permission sets, action groups define what actions users can or can't perform. If action groups don't have an accompanying user group and authorization policy, you can't enforce and automatically update information in the action groups.

The **Migrate Adaptive Planning Permission Sets and Assignments** task will automatically create action groups and authorization policies based on permissions and user information in Adaptive Planning. If after consulting the **User Permissions Comparison Report**, you find that user/permission information don't match, you can use these tasks to create, edit, and verify action groups:

- **Create Action Group**
- **Edit Action Group**
- **View Action Group**

User Groups

Also known as security groups, user groups are collections of users with similar roles or assignments that give them access to secured items or business objects within an organization. Using UAM, you can assign user groups to action groups, by linking them with an authorization policy. Currently, role-based, user-based, and integration system security groups are the only types of security group enabled for use as user groups.

You can also access the **Subscribe User Groups to Adaptive Planning** task to sync user groups with Adaptive Planning. This task enables you to populate Adaptive Planning with up-to-date group and user information.

Authorization Policies

Referred to as permission set assignments in Adaptive Planning, authorization policies link action groups and user groups. Users can be members of multiple groups and authorization policies in UAM.

You can access the **Create Authorization Policy** task to configure an authorization policy, ensuring that changes to actions or user assignments automatically sync across Workday and Adaptive Planning. You can also access the **Edit Authorization Policy** task to modify existing policies, including the*Name*, *Description*, *Action Groups*, and *User Groups* associated with a policy.

UAM Reports

As you navigate each step and configure individual features in UAM, you can reference reports to ensure users or permissions match across Workday and Adaptive Planning:

- **User Permissions Comparison Report** indicates whether the permissions for a specific user match across Workday and Adaptive Planning. If a user's permissions don't match, the report will show *Additional Permissions* for Workday or Adaptive Planning, identifying the permissions without an equivalent action in Workday.
- **View Action Group Details** enables you to confirm that action groups, actions, policies, and users are associated with one another and tied to the appropriate Adaptive Planning application instance. You can use this report at any stage of the UAM setup process, including for troubleshooting.

Related Information
Examples
Feature Release Note: Unified Access Management (UAM)

Data Privacy

Data Masking

Concept: Masking Sensitive Data

You can mask sensitive data in your tenant. Example: For identity theft protection. You can mask data by:

- User account.
- Security group.
- Files uploaded before a selected date and time.

Data masking either masks or substitutes placeholder values for actual values to hide data from Workday users. Data masking also hides profile pictures from these users. Workday automatically enables data masking for the wd-support account.

You can use the data masking feature in your Sandbox, Production, or Implementation tenant. Because this feature doesn't allow updating, use it with caution when enabling it in Production.

Data masking excludes access to certain Workday functionality as well as functionality that requires connecting to another service, including:

- Business form printing.
- Integrations, including:
  - Graph API (for Extend customers).
  - Reports as a Service.
  - REST API.
  - Workday Studio.
- Scheduled reports.
- Access to documents in **My Reports**.
- Solutions.

Workday enforces data masking in a proxy session if you:

- Enable data masking and then start a proxy session.
- Start a proxy session on behalf of a Workday account that enables data masking.

You can apply data masking to all outbound data for specified Workday accounts and security groups, including:

- Reports shown in the user interface.
- Exported report data.
- Integration output.

To select categories of data to mask, access the **Manage Data Sensitivity** task.

Data masking affects several hundred fields throughout Workday that contain, or derive values from, any of these sensitive data groups for a worker:

- Bank Account Number.
- Person Birth Place.
- Person Date of Birth.

- Person Global Identifier.
- Tax ID.
- Healthcare Information.

Workday applies these restrictions when displaying data to individual Workday accounts and security groups with data masking enabled:

- ***** replaces text values in fields.
- 01/01/2020 or ***** replaces date values.
- ***** replaces numeric values.
- Profile pictures are hidden.
- You can't save changes if any field contains sensitive data.

Workday imposes these additional access restrictions on user accounts and security groups with data masking enabled:

- Users and security groups with masked accounts can't download attachments from **My Reports**. You can, however, exempt accounts and security groups from this restriction in the **Allow File Access for** section of the **Enable/Disable Data Masking** task. Filenames for attachments display as asterisks and aren’t hyperlinks.
- Users and security groups with masked accounts can't modify their data if it's masked. Example: They can't use the **Correct My Birth Date** task to change their birth date if **Person Date of Birth** is selected on the **Manage Data Sensitivity** task.
- Users with masked accounts can't access a facet for an indexed search if that facet references an attribute or relationship marked as sensitive data. Example: The facet **Age Group** references the sensitive data group **Person Date of Birth**.

In the **All Workday Accounts** report, the **Sensitive Data is Masked in Output** field returns **Yes** if data masking is enabled.

Note: You might encounter an *Instance ID cannot be parsed* error when data masking is enabled and you attempt to modify data in certain circumstances.

Example: A user attempts to change a global preference when data masking is enabled for that user's account. If you encounter the error, disable data masking, make the desired changes in Workday, and then reenable data masking.

Enable or Disable Data Masking

Prerequisites

Access the **Manage Data Sensitivity** task to select the sensitive data groups to mask.

Security: *Security Administration* domain in the System functional area.

Context

Data masking either masks or substitutes placeholder values for actual values to hide data from Workday users. You can apply data masking to all outbound data for specified Workday accounts and security groups, including:

- Reports shown in the user interface.
- Exported report data.
- Integration output.

You can't use the **Edit Workday Account** task to enable or disable data masking for a Workday account, but you can use the **Enable/Disable Account Data Masking** task to enable or disable data masking for an account.

Note: You might encounter an *Instance ID cannot be parsed* error when data masking is enabled and you attempt to modify data in certain circumstances.

Example: A user attempts to change a global preference when data masking is enabled for that user's account. If you encounter the error, disable data masking, make the desired changes in Workday, and then reenable data masking.

Steps

1. Access the **Enable/Disable Data Masking** task.
2. As you complete the task, consider:

Option	Description
Enable Data Masking for	Data masking applies for these selected users and security groups.
Allow File Access for	Selected users and security groups can access all files from **My Reports**.
Allow File Access for these Masked Accounts only for Files Uploaded after this Date and Time and Timezone	Selected users and security groups can access files from **My Reports** that were uploaded after this date, time, and time zone.
Disable Data Masking for Internal User of Proxy Account	Users are exempt from data masking. Example: Accounts used for Workday internal support.

Result

Workday applies masking restrictions on user accounts and security groups that have data masking enabled.

Related Information
Concepts
Concept: Masking Sensitive Data on page 274

Data Purging

Setup Considerations: Data Purging

You can use this topic to help make decisions when planning your configuration and use of data purging. It explains:

- Why to set it up.
- How it fits into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What It Is

Data purging in Workday enables you to delete certain personally identifiable information (PII) permanently from your tenant.

Business Benefits

The data purging feature helps you comply with privacy regulations and data protection laws. Example: General Data Protection Regulation (GDPR) requirements.

Use Cases

- Purge data for selected groups of users on an ad hoc basis. Example: Purge worker responses to questionnaires and surveys.
- Periodically purge well-defined sets of user data after a predefined time period. Example: Purge personal data for workers whose contracts ended 5 years ago.

Questions to Consider

Question	Considerations
Will you need the data you're purging later?	Data you purge from the tenant using the data purging feature is permanent and irreversible. You can't recover the data. If you want to retain data in the tenant but protect it, you might be able to use the data masking feature. Data masking masks certain sensitive data so it's visible only by selected accounts and security groups. It's available only for a limited number of sensitive data fields.
For which objects do you want to purge data?	You can use the data purging feature to purge information related to these objects in Workday: • Candidate • Case • Customers • Education Test Result • Extended Enterprise Learner • External Case Creator • Former Worker • Job Application • Learning Instructor • Pre-Hire • Questionnaire Response • Referee • Student • Student Engagement Note • Student External Transcript • Student Document • Supplier • Worker You can also purge attachments on multiple financial entities. Workday also contains functionality, separate from the data purging feature, for purging certain other information. Example: Notifications for users and academic affiliates.
What data do you need to purge?	The data purging feature enables you to purge predefined sets of data, called Purgeable Data Types (PDTs) for given entities. Example: Union membership data for active workers. The PDTs

Question	Considerations
	available depend on the entity that you want to purge.
Do you need to purge the same data periodically or on a regular basis?	You can predefine the data that you want to purge and save it in a reusable purge plan. Purge plans are optional. If you want to perform a one-time, ad hoc data purge, you can run a purge operation without a purge plan. You can then select the specific data you want to purge.

Recommendations

- Test data purging in your Sandbox environment before you purge data in your Production environment.
- Run your custom report before you purge data and ensure it returns the correct list of entities for which you want to purge data.
- Create your custom report so that it contains the same data that you want to purge using the data purging process. You can then run the report before and after the purge and compare the results to verify that Workday purged the data.
- Use purge plans when you periodically need to purge well-defined sets of user data (Example: Personal data for terminated workers).
- Only grant the ability to purge data to users who understand the purging process and its consequences. Typically, security administrators perform data purges.
- Schedule purge operations during periods of low tenant use. Example: 3:00 AM Sunday.
- Limit purging to no more than 25,000 instances at a time, and enable 1 purge operation to complete before starting another. Purging spawns individual jobs for each person impacted by the purge, and 25,000 is the threshold for the total number of these jobs running concurrently.

Requirements

The person running **Purge Person Data** must have unconstrained access to all resulting rows, columns, and fields that the custom report used by the task might return.

Limitations

Workday doesn't support purge plans for purging recruiting candidates.

You can purge only data for a *Pre-Hire* when:

- The Pre-Hire is created as a standalone Pre-Hire.
- There's no active, terminated, or former *Candidate*, *Student*, or *Worker* record linked to the Pre-Hire.
- The Pre-Hire doesn't have complete or in-progress *Hire* events.
- The Pre-Hire doesn't have incomplete events.

Tenant Setup

- Financial regulations often mandate the retention of personal information, such as names on expense receipts, for a longer period than personal data regulations. Use the **Years to Retain Financial Data for Purged Workers** field on the **Edit Tenant Setup - Financials** task to preserve financial data for the set number of years regardless of the privacy purge settings.
- Use the **Purging Warning Message** field on the **Edit Tenant Setup - System** task to set up a custom warning message. The message displays in addition to the standard disclaimer when a user confirms a purge of person data.

Security

These domains in the System functional area:

Domains	Considerations
Custom Report Creation *Manage: All Custom Reports* *Report Tag Management*	Enables users to create and manage the custom reports that Workday uses to specify entities (Example: inactive suppliers) for which they want to purge data.
Purge Person Data	Enables users to create and manage purge plans, purge privacy data, and run related reports.
Purge Single Entity Data	Enables users to purge privacy data for a single entity from the related actions menu. Example: A single candidate.
Purge Supplier (Subdomain of the *Purge Person Data* domain.)	Enables security groups to create and manage purge plans, and purge privacy data for suppliers.
Mass Operation Management	Enables users to use the Mass Operation Management task to schedule purge operations.
Set Up: Tenant Setup - System	Enables users to specify a custom purging warning message to display before a data purging operation.
Security Configuration	Enables users to set up segment-based security groups.

You can't use role security to limit the scope of purging. You can, however, use the sharing options of the custom report to control the users who can see it.

Business Processes

No impact.

Reporting

Reports	Considerations
Purge Person Data Job Monitor	Use this report to view the status of *Mark Person Data for Purge* jobs, which execute instance data purges for each PDT selected on: • Single specified instances. • All instances returned by the report specified by the user.
Scheduled Future Processes	Use this report to manage scheduled privacy purge operations.

Integrations

No impact.

Connections and Touchpoints

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Related Information
Reference
Reference: Purgeable Data Types on page 287

Steps: Purge Person Privacy Data

Context

You can permanently purge certain personally identifiable information (PII) from your Workday tenant for certain entities. Examples:

- Active workers.
- Candidates.
- Pre-Hires.
- Prospects.
- Student Documents.
- Suppliers.
- Terminated workers.

Workday purges personally identifiable information for the entities that you identify in a custom report. You can:

- Create a custom report to identify the entities for which you want to purge personal data.
- Use a custom report you previously created if it meets your criteria.

Note: Workday can't reverse or roll back the deletion in your tenant. Only purge the data that you've tested and confirmed in Sandbox that you no longer need.

Steps

1. Create a Privacy Purge Custom Report on page 285.

   Workday requires a privacy purge custom report to purge privacy data. The report generates a list of entities for which you want to purge data from the tenant. You can use a custom report you previously created if it meets your criteria.

   Note: Workday generates and saves a purge summary report after every purge operation. Workday captures and persists any filter conditions you include in your privacy purge custom reports in the purge summary reports for the life of the tenant. We recommend that you don't include filter conditions in your custom report that overtly identify individuals. Example: Filter on employee ID rather than employee name or email address, as employee IDs are more discreet.
2. (Optional) Access the **Create Purge Plan** task.

   Create a plan that identifies the data types you want to purge. As you complete the task, consider:

Option	Description
Object to Purge	When you copy an existing purge plan, the new plan inherits the object from the existing plan.
Custom Report Definition for Purge Plan	(Optional) A custom report definition that is based on the same business object as the **Object to Purge**. Selecting a custom report here saves it with the purge plan.

Option	Description
Purgeable Data Type (grid)	Select the check boxes for the purgeable data types that you want to purge.
Select All	Selects all purgeable data types in the grid except for those data types for active workers, unless you also select **Purge Active Worker Data Only**.
Purge Active Worker Data Only	Deactivates the purgeable data types that are for terminated workers. This check box only displays when the **Object to Purge** is Worker.

Security:

- *Purge Person Data* domain in the System functional area.
- *Purge Supplier* domain as a subdomain of the *Purge Person Data* domain.

3. (Optional) Access the **Edit Tenant Setup - System** task.

   Enter a custom message in the **Purging Warning Message** field. This message displays above, and in addition to, the standard disclaimer when you confirm a purge of person data.

   Security: *Set Up: Tenant Setup - System* domain in the System functional area.

4. Access the **Purge Person Data** task and select a privacy purge custom report in the **Population to Purge (Report Definition)** field.
5. As you complete the remainder of the task, consider:

Option	Description
Purge Plan	(Optional) Displays only the purgeable data types in the grid for the purge plan that you select. When you don't select a purge plan, you can select from any of the purgeable data types that are available for the displayed class name.
View report on selected population	(Optional) Open this link in a new tab to review the persons for whom you are deleting data.
Select All	Selects all purgeable data types in the grid except for those data types for active workers, unless you also select **Purge Active Worker Data Only**.
Purge Active Worker Data Only	Deactivates the purgeable data types that are for terminated workers. This check box only displays when the **Class Name of Instances to be Purged** is Worker.
Include Custom Objects for Purging	(Optional) Select to purge all custom objects associated with the specified worker population when you purge PII that is associated with those workers. Example: You purge gender and age from the profiles of a worker population. Workday also purges all custom objects on the **Additional Data** tab of their profiles.
Purge date-driven items dated	If any selected Purgeable Data Types also have the **Is Date-Driven** check box selected, you might need to complete 1 or more of these fields: • **On**: Purges only items dated on the selected date.

Option	Description
	• **On or before**: Purges any items dated on or before the selected date. • **Inclusive in-between from** and **Inclusive in-between to**: Purges items dated within a range consisting of these dates, inclusive.

Security:

- *Purge Person Data* domain in the System functional area.
- *Purge Supplier* domain as a subdomain of the *Purge Person Data* domain.

6. Click **OK**, select the **Confirm** check box and click **OK** to start the purge process.

Result

Workday permanently deletes the data from your tenant for the population that the custom report returns at the time you confirm the purge.

Next Steps

- Use the *Person Purged* report field to exclude purged persons from reports using these data sources:
- • All Active and Terminated Workers.
  • Prospects and Candidates for Purging.
- Use the **Purge Person Data Job Monitor** report to:
  - Track the progress of *Mark Person Data for Purge* concurrent jobs.
  - Abort *Mark Person Data for Purge* concurrent jobs that are still processing in the background.
  - Access the **Purge Summary Report** for specific purge jobs.

The **Purge Summary Report** displays purge information for candidate or worker purges, including:

- The date and time when a purge was initiated.
- Who submitted the purge.
- Purgeable data types selected for purging.
- Details of the single entity purge, or custom report used for the purge.
- Purgeable entities that were successful or ineligible for purging.

The **Purge Summary Report** is secured to the *Purge Person Data* domain.

Note: Workday restricts access to the **Purge Summary Report** based on a user's access to both the:

- Data source specified in the privacy purge custom report.
- Privacy purge custom report used in the purge operation.

If a user doesn't have access to both of these items, then they won't see a link to the **Purge Summary Report** in the **Purge Person Data Job Monitor**, or be able to open the report if they are provided with a link to it by another user.

Related Information
Reference

Reference: Purgeable Data Types on page 287

The Next Level: Data Purging

Steps: Schedule Privacy Purge Operations

Context

You can schedule a privacy purge to run periodically. Example: When local law requires you to purge certain types of personal data after a predefined time period.

Note: Workday doesn't support purging some entities using a scheduled privacy purge operation.

Steps

1. Create a Segment-Based Security Group for Mass Operations.
   Create the segment-based security group with:
   - **Security Groups**: Security groups that will approve the privacy purge operation.
   - **Access to Segments**: *Purge Person Data*.
2. From the related actions menu of the segment-based security group, select:
   a. **Security Group** > **Maintain Domain Permissions for Security Group**.
   b. **Mass Operation Management** in the **Domain Security Policies permitting Modify access** field.
3. Activate Pending Security Policy Changes on page 203.
4. Create a Privacy Purge Custom Report on page 285.
   Workday requires a privacy purge custom report to purge person privacy data. The report generates a list of entities for which you want to purge data from the tenant. You can use a custom report you previously created if it meets your criteria.
5. (Optional) Access the **Create Purge Plan** task.
   Create a plan that identifies the data types you want to purge. As you complete the task, consider:

Option	Description
Object to Purge	When you copy an existing purge plan, the new plan inherits the object from the existing plan.
Custom Report Definition for Purge Plan	(Optional) A custom report definition that is based on the same business object as the **Object to Purge**. Selecting a custom report here saves it with the purge plan.
Purgeable Data Type (grid)	Select the check boxes for the purgeable data types that you want to purge.
Select All	Selects all purgeable data types in the grid except for those data types for active workers, unless you also select **Purge Active Worker Data Only**.
Purge Active Worker Data Only	Deactivates the purgeable data types that are for terminated workers. This check box only displays when **Object to Purge** is Worker.

   Security:
   - *Purge Person Data* domain in the System functional area.
   - *Purge Supplier* domain as a subdomain of the *Purge Person Data* domain.
6. Access the **Mass Operation Management** task.
   As you complete the task, consider:

Option	Description
Mass Operation Type	Select *Role Data Purge Operation Type*.

Option	Description
Input Report	Select the privacy purge custom report that you created earlier.
Run Frequency	Schedule the privacy purge operation to run at times of low usage. **Note:** If you select *Run Now* for **Run Frequency**, the **Mass Operation Configuration** and **Schedule** tabs in the remainder of the task don't display.

Security: *Mass Operation Management* domain in the System functional area.

7. Click **OK**, then complete the fields on the **Mass Operation Configuration** tab:
   The tab doesn't display if you select *Run Now* for **Run Frequency**, but the fields do display.

Option	Description
Purge Plan	(Optional) Displays only the purgeable data types in the grid for the purge plan that you select. When you don't select a purge plan, you can select from any of the purgeable data types that are available for the **Primary Business Object** named in the privacy purge custom report.
Purgeable Data Type (grid)	If you don't select a purge plan, select the check boxes for data types you want to purge. Workday automatically purges some data types.
Select All	Selects all purgeable data types in the grid except for those data types for active workers, unless you also select **Purge Active Worker Data Only**.
Purge Active Worker Data Only	(Optional) Select to purge data types that are relevant to active workers. This check box only displays when the **Primary Business Object** named in the custom report is Worker.
Include Custom Objects for Purging	(Optional) Select to purge all custom objects associated with the specified worker population when you purge PII that's associated with those workers. Example: You purge gender and age from the profiles of a worker population. Workday also purges all custom objects on the **Additional Data** tab of their profiles.
Purge date-driven items dated	If any selected Purgeable Data Types also have the **Is Date-Driven** check box selected, you might need to complete 1 or more of these fields: • **On**: Purges only items dated on the selected date. • **On or before**: Purges any items dated on or before the selected date. • **Inclusive in-between from** and **Inclusive in-between to**: Purges items dated within a range consisting of these dates, inclusive.

Option	Description
Review Notification Settings	Workday sends a notification to the processing user and optional additional users, enabling them to abort or continue the purge operation. The **Delay** determines the amount of time the users have to review and act on the notification before the default action occurs. For privacy purge operations, you can only select *Abort Mass Action* as the **Default Review Action**.
Report Definition	The report definition grid in this section shouldn't contain any fields.

8. If you selected anything other than *Run Now* for **Run Frequency**, complete the settings on the **Schedule** tab.

Result

Workday enables the privacy purge to run as a mass operation when needed or as a scheduled background process. Workday sends a notification to the processing user and any other users specified in the **Review Notification Settings** section, either immediately or at the scheduled time as determined by the **Run Frequency**. If none of the users continue with the operation before the **Delay** period expires, the operation automatically aborts.

The **Mass Operation Management** task limits the number of actions that Workday performs in a single execution. The base of this limitation is the number of instances the custom report generates. For a Role Data Purge Operation Type, the limit is 50,000 instances.

Next Steps

Access the **Scheduled Future Processes** report to manage scheduled privacy purge operations. Examples: You can:

- Edit a scheduled occurrence of a scheduled privacy purge operation.
- Suspend a scheduled privacy purge operation.

Related Information
Tasks
Manage Scheduled Future Processes
Reference
Reference: Purgeable Data Types on page 287
The Next Level: Data Purging

Create a Privacy Purge Custom Report

Prerequisites

Security: These domains in the System functional area:

- *Custom Report Creation*
- *Manage: All Custom Reports*
- *Report Tag Management*

Context

You can create an advanced custom report that generates a list of entities for which you want to purge data from the tenant. Examples: People or inactive suppliers.

Note: The Workday account must have unconstrained access to all secured items used by the report.

Steps

1. Access the **Create Custom Report** task.
   As you complete the task, consider:

Option	Description
Report Type	Select *Advanced*.
Optimized for Performance	Clear this check box.
Data Source	Select a report data source based on the *business object* you want to purge. Examples: Worker, Former Worker, Supplier, or Candidate.

2. On the **Edit Custom Report** task for your custom report, select *Purge* under **Report Tags** to select the purge tag.
3. As you complete the **Columns** tab:
   a. Include at least 1 field in the report to identify the entities for which you want to purge personal data. Example: The *First Name* and *Last Name* fields on the *Worker* business object.
   b. (Optional) To purge only prospects or candidates attached to purged terminated workers, include the *Person was Purged* field in the report.
4. (Optional) If you'll use the report to schedule privacy purge operations, complete the **Filter on Instances** section on the **Filter** tab. Filter on instances where the:
   - **Is Eligible for Active Purge** field is equal to Yes, if the report might be used to schedule an active worker data purge.
   - **Is Eligible for Purge** field is equal to Yes, if the report might be used to schedule any other worker data purge.
5. On the **Prompts** tab, ensure that the report doesn't include prompts that require user input when it runs.

Next Steps

You can run the report and ensure it returns the correct list of entities for which you want to purge personal data.

Related Information
Tasks
Steps: Create Advanced Reports
Reference
The Next Level: Data Purging

Reference: Auditing Purged Person Data

The **Purge Person Data** task provides an audit trail. It tracks:

- Who ran the task and when.
- The data types selected.
- The report used to select the purged population.
- The number of workers whose data Workday purged.

To determine	Run...	Enter Task as...
Who ran the task	View User Activity, View User or Task or Object Audit Trail	Purge Person Data

To determine	Run...	Enter Task as...
The areas selected to be purged	View User or Task or Object Audit Trail	Purge Person Data
The report used for the purge	View User or Task or Object Audit Trail	Purge Person Data

Related Information
Reference
The Next Level: Data Purging

Reference: Purgeable Data Types

Purgeable Data Types (PDTs) are related to these entities in Workday:

- Active Workers on page 287
- Candidates on page 290
- Case on page 295
- Customers on page 296
- External Learning Assessor on page 297
- External Learning Instructor on page 297
- Extended Enterprise Learner on page 298
- Financial Entities on page 298
- Former Workers on page 301
- Job Applications on page 306
- National IDs on page 308
- Payroll
- Pre-Hires on page 308
- Questionnaire and Survey Responses on page 310
- Student on page 310
- Student Documents on page 311
- Student Immigration Data on page 313
- Tax Elections on page 313
- Terminees on page 313

Active Workers

Purgeable Data Type	Description
Audio Pronunciation	Purges audio name pronunciation data.
National IDs	Purges: • Identifier series • Issuing Agency • National ID type • Issue Date • Expiration Date • Issued by • Comments
Personal Information - Ethnicity	Purges: • Ethnicity • Hispanic or Latino

Purgeable Data Type	Description
	• Ethnicity Visual Survey
Personal Information: Country Specific Section 1	Purges: • Country Specific Section 1 - Field 1 • Country Specific Section 1 - Field 2 • Country Specific Section 1 - Field 3
Personal Information: Country Specific Section 2	Purges: • Country Specific Section 2 - Field 1 • Country Specific Section 2 - Field 2 • Country Specific Section 2 - Field 3
Personal Information: Country Specific Section 3	Purges: • Country Specific Section 3 - Field 1 • Country Specific Section 3 - Field 2 • Country Specific Section 3 - Field 3
Personal Information: Non Country Specific Section 1	Purges: • Non Country Specific Section 1 - Field 1 • Non Country Specific Section 2- Field 2 • Non Country Specific Section 3 - Field 3
Personal Information: Non Country Specific Section 2	Purges: • Non Country Specific Section 2 - Field 1 • Non Country Specific Section 2 - Field 2 • Non Country Specific Section 2 - Field 3
Personal Information: Non Country Specific Section 3	Purges: • Non Country Specific Section 3 - Field 1 • Non Country Specific Section 3 - Field 2 • Non Country Specific Section 3 - Field 3
Phonetic Pronunciation	Purges phonetic name pronunciation data.
Self-Identification - Sexual Orientation, Gender Identity, Pronoun	Purges: • Sexual Orientation and Gender Identity • Sexual Orientation • Gender Identity • Pronoun
Talent - Check Ins and Check In Topics	Purges: • Check Ins • Check Ins Attachments • Check In Topics • Check In Topics Attachments
Talent - Feedback for Active Workers	Purges: • Anytime feedback (per request or otherwise) • Feedback Given

Purgeable Data Type	Description
	• Feedback Requested
Talent - Performance Improvement Plans (PIPs) and Disciplinary Actions (DAs)	Purges: • BP Comments • Component Evaluation • Content Evaluation • Evaluation Event • Goals Review • Manager Evaluation • Ratings • Review Comments (Answers, Responses) • Review Section • Section Evaluation Rating • Supporting documents Select a date range when purging PIPs and DAs. Workday includes the PIPs and DAs that have an end date for the review period falling within the date range in the purge.
Talent - Performance Reviews and Development Plans	Purges: • BP Comments • Component Evaluation • Content Evaluation • Evaluation Event • Goals Review • Manager Evaluation • Review Section • Ratings • Comments • Supporting documents Select a date range when purging Performance Reviews and Development Plans. Workday includes the Performance Reviews and Development Plans that have an end date for the review period falling within the date range in the purge.
Union Membership	Purges: • Comments • Member of Union • Membership end date • Membership start date • Seniority Date • Union Seniority Date • Union Type
Universal ID	Purges Person Universal Identifier.
Vaccinations	Purges: • Attestation e-signature moment

Purgeable Data Type	Description
	• Attachments on Add Vaccination Event • Comments • Vaccination Date • Vaccination Status • Vaccine • Vaccine Type To purge the vaccinations data, select the **Purge Active Worker Data Only** check box in the purge plan, not in the **Purge Person Data** task.
Workplace Test	Purges: • Attachments on Add Workplace Test Event • Comments • Workplace Test Result • Workplace Test Taken Date • Workplace Test Type

Candidates

Some purgeable data types for candidates require a purge plan and only apply to certain person types.

Purgeable Data Type	Purge Plan	Person Types	Description
Added Documents	Optional	Candidates	Any additional documents added using the **Add Documents** task. When you purge a candidate who has a worker profile with candidate documents, Workday removes the candidate documents from the worker profile.
Awaiting Action for Prospects and Candidates	Optional	• Candidates • Prospects	Purges events awaiting action.
Candidate and Job Application - Social Share	Optional	• Candidates • Prospects	Purges data related to social share.
Candidate Notes	Optional	• Candidates • Prospects	Purges all the notes content associated with the candidate and their job applications. Purges all the notes content associated with the prospect.
Contact Information	Required	• Candidates	Purges data related to the:

Purgeable Data Type	Purge Plan	Person Types	Description
		• Former Workers • Terminated Workers	• Address. • Email address. • Instant messenger. • Phone number. • Social network. • Web address.
Financials - Expense Reports	Optional	Candidates	Purges: • Any memos on the expense report header and line items. • The file, filename, and comments on any attachments.
Interview	Optional	• Candidates • Prospects	Purges interview events, comments, questionnaires, and sessions.
Job Alerts, Internal Candidates	Optional	Candidates	Purges the Job Alert Preferences for an Internal Candidate.
Names	Required	• Candidates • Former Workers • Terminated Workers	Purges data related to: • Additional names. • All name types. • Local person names. • Preferred names.
Person IDs	Required	• Candidates • Former Workers • Terminated Workers	Purges these ID types: • Contingent Worker • Custom • Employee • Former Worker • Government • License • National • Passport • Reference ID • Visa Purges this ID data: • Comment • Expiration Date • ID • Identifier Series • Issued by Country • Issued Date • Issuing Authority

Purgeable Data Type	Purge Plan	Person Types	Description
			• License Class • License ID Type • Verification Date • Verified by Worker
Prospect and Candidate Activity Stream Comments	Required	Candidates	Purges data related to: • Activity stream comments. • Custom notification events. • Notifications when tagging someone in the activity stream.
Prospect and Candidate Education	Optional	Candidates	Purges this data related to education: • Associated Skills • Candidate Degree • Fields of Study • Schools
Prospect and Candidate Event Comments	Required	Candidates	Purges this data related to event comments: • Background check comments. • Competency. • Endorsements. • Event comments. • Message notifications such as push notifications. • Notification content. • Notification events. • Personal Notes. • Recruiting Assessment. • Recruiting emails. • Referred By. • Resume Summary.
Prospect and Candidate Experience	Optional	Candidates	Purges this data related to experience: • Average Year Per Job • Business Title • Comment • Company • Country • Country Region • Currently Work Here

Purgeable Data Type	Purge Plan	Person Types	Description
			• End Month • End Year • Experience End Date • Experience Start Date • ID • Job Title • Location Name • Prospect Company • Prospect Job Title • Responsibilities and Achievements • Skill • Start Month • Start Year • Time in Current Job • Total Years Experience • Years in Current Job
Prospect and Candidate Personal Information	Required	Candidates	Purges this data related to personal information: • Attachments. • Comments. • Duplicate Resolution. • Email. • Image Name. • Phone. • Previous Email. • Previous Worker. • Previous Worker ID. • Previous Worker Location. • Previous Manager. • Social Network Account. • Web Address. • Generated documents, including eSignature. • Attachments added to business processes.
Prospect and Candidate Shared Messages	Required	Candidates	Purges notes, comments, and messages shared with other workers by recruiters or hiring managers.

Purgeable Data Type	Purge Plan	Person Types	Description
Purge LinkedIn Person Data	Optional	Candidates	Purges the LinkedIn person, their attributes, and the link between the LinkedIn person and the candidate or worker. Also removes the relationship between the LinkedIn person's 1-Click Export record and the recruiter LinkedIn person.
Questionnaire Results	Required	Candidates	Purges questionnaire answers, scores, and attachments.
Recruiting Campaign Communications	Required	Candidates	The content of emails sent as part of recruiting campaigns.
Recruiting Campaign Communications for Job Applications	Optional	Candidates	The link between recruiting campaigns and the job applications submitted by campaign recipients. When you purge this link, Workday no longer counts purged applications in campaign analytics reports.
Recruiting Communications	Required	Candidates	Purges notification content for: • Notes • SMS from conversational messaging • Attachments for Send Message and Invite to Apply • Recruiting email attachments • Conversation Messages • Conversation Participants • Candidate SMS Notifications • Recruiting Notification Events • Notification Generated Documents

Purgeable Data Type	Purge Plan	Person Types	Description
Recruiting Reminders	Optional	• Candidates • Prospects	Purges personal reminders.
Recruiting System User	Required	Candidates	Purges the System User (Name) for the candidate.
Worker Recruiting Candidate Reminder	Optional	Candidates	Purges candidate reminders, notes, and notifications for a worker.

Case

Workday enables you to purge individual cases by selecting the *Cases For Purge* **Data Source** on your custom report.

Purgeable Data Type	Purge Person Data Task without Plan	Applies To	Description
Case Details	Optional	Active Workers, Terminees	Purges this data related to case details: • Comments. • Internal Notes. • Description. • Title. • Attachments. • Creator Name. • Created For. • Created About. • Employee Name. • External Reference ID. • Email From. • Events. • Follow-Up Dates.
Case Events for Worker	Optional	Active Workers, Terminees	Purges this data related to case events: • Comments. • Notification Event. • Questionnaire Answer. • Questionnaire Attachments. • Questionnaire Response. • Workflow Email Events.
Case Notifications	Optional	Active Workers, Terminees	Purges this data related to case notifications:

Purgeable Data Type	Purge Person Data Task without Plan	Applies To	Description
			• All Notifications.
Case Questionnaires	Optional	Active Workers, Terminees	Purges this data related to case questionnaires: • Answers. • Attachments. • Response.
External Case Creator	Optional	Active Workers, Terminees	Purges this data related to external case creator: • Email Address. • Name.

Customers

A purge plan is optional when you purge customer data.

To purge data related to Renewals, ensure you select the **Include Custom Objects for Purging**check box.

Purgeable Data Type	Description
Customer Attachments	Purges data related to customer attachments.
Customer Contact Information	Purges this data related to customer contact information: • Addresses • Email • Instant Messenger Address • Phone • Web Address
Customer Contacts	Purges data related to contact persons and this data related to their contact information: • Addresses • Email • Instant Messenger Address • Phone • Web Address
Customer Credit Card Profiles	Purges data related to customer credit card profiles.
Customer DUNS Number	Purges data related to customer DUNS number.
Customer Group	Purges data related to customer group.
Customer IDs	Purges this data related to customer IDs: • Customer ID • Customer Reference ID • Government-Issued Customer ID • Intermediary/Vendor ID • Vendor-Issued Customer ID

Purgeable Data Type	Description
Customer Lockboxes	Purges data related to customer lockboxes.
Customer Name	Purges this data related to customer name: • Alternate Name • Business Entity Name • Business Entity Phonetic Name • Customer Name • Indexed Name
Customer Notes	Purges data related to customer notes.
Customer Tax ID	Purges data related to customer identification number.
Questionnaire Results	Purges data related to questionnaire results.
Settlement Bank Accounts	Purges data related to settlement bank accounts.

External Learning Assessor

Purgeable Data Type	Report Data Source	Description
Contact Information	*Learning Trainer*	Purges person's contact information and related events.
Names	*Learning Trainer*	Purges: • Additional name. • Legal name. • Preferred name.
Personal Information	*Learning Trainer*	Purges: • Worker's personal information. • Pre-Hire's personal information.
(Optional) System	*Learning Trainer*	Purges: • Person's signons. • Person's username.

External Learning Instructor

Purgeable Data Type	Report Data Source	Description
Contact Information	*Learning Instructors*	Purges person's contact information and related events.
Names	*Learning Instructors*	Purges: • Additional name. • Legal name. • Preferred name.
Personal Information	*Learning Instructors*	Purges: • Worker's personal information.

Purgeable Data Type	Report Data Source	Description
		• Pre-Hire's personal information.
(Optional) System	*Learning Instructors*	Purges: • Person's signons. • Person's username.

Extended Enterprise Learner

Purgeable Data Type	Report Data Source	Description
Contact Information	*Extended Enterprise Learners*	Purges person's contact information and related events.
Names	*Extended Enterprise Learners*	Purges: • Additional name. • Legal name. • Preferred name.
Personal Information	*Extended Enterprise Learners*	Purges: • Worker's personal information. • Pre-Hire's personal information.
(Optional) System	*Extended Enterprise Learners*	Purgers: • Person's signons. • Person's username.

Financial Entities

Workday enables you to purge attachments on multiple financial entities. A purge plan is optional when you purge financial attachments.

After you purge attachments:

- You can still see that there were attachments on financial entities.
- You can’t view details about or download these attachments, and Workday no longer stores this information.

Object to Purge	Financial Entities with Purgeable Attachments	Report Data Source
1099 MISC Adjustment	1099 Adjustments	**1099 Adjustment**
Abstract Supplemental Data	Supplemental Data	**Supplemental Data**
Account Certification	Account Certifications	**Account Certifications**
Accounting Adjustment	Accounting Adjustments	**Accounting Adjustment**
Accounting Center Detailed Journal	Accounting Center Detailed Journals	**Accounting Center Detailed Journal**
Ad Hoc Bank Transaction	Ad Hoc Bank Transactions	**Ad Hoc Bank Transactions**
Ad Hoc Payee	Ad Hoc Payees	**Ad hoc Payees**

Object to Purge	Financial Entities with Purgeable Attachments	Report Data Source
Ad Hoc Payment Template	Ad Hoc Payment Templates	**Ad Hoc Payment Template**
Ad Hoc Payment	Ad Hoc Payments	**Ad Hoc Payments**
Advanced Ship Notice	Advanced Ship Notices	**Advanced Ship Notices**
Allocation Definition	Allocation Definitions	**Allocation Definition**
Allocation Plan	Allocation Plans	**Allocation Plans**
Allocation Pool	Allocation Pools	**Allocation Pools**
Bank Account	Bank Accounts and Bank Account Changes	**Bank Accounts**
Bank Account Transfer	Bank Account Transfers	**Bank Account Transfers**
Bank Account Transfer for Settlement	Bank Account Transfers for Settlement	**Bank Account Transfers for Settlement**
Bank Fee Service Contract	Bank Fee Service Contracts	**Bank fee service contract**
Bank Fee Statement	Bank Fee Statements	**Bank Fee Statements**
Bank Statement	Bank Statements	**Bank Statements**
Billing Schedule Attachments	Billing Schedule	**Billing Schedules**
Budget	Budget Entries and Budget Amendments	**Plans**
Business Asset	Business Assets	**Business Assets** You can add the **Has Attachment** report field to filter business assets with attachments.
Cash Pool	Cash Pools	**Cash Pool**
Company Ownership Details	Company Ownership Details	**Company Ownership Details**
Customer Contract and Related Attachments	Customer Contract	**Customer Contracts**
Customer Contract Checklist Task Attachments	Customer Contract Checklist Template	**Customer Contract Checklist Templates**
Direct Debit Mandate	Direct Debit Mandates	**Direct Debit Mandates**
Dock Logging Manifest Line	Dock Logging Manifest Lines	**Manifest Line**
Donor Contribution	Donor Contributions	**Donor Contributions**
External Supplier Request	External Supplier Requests	**External Supplier Requests**
External Supplier Site	External Supplier Sites	**External Supplier Sites**
Financial Event	Supplier Alternate Name Change Events and Supplier Contact Information Change Events	**Supplier Business Process Transactions with Purgeable Attachments**
Gift	Gifts	**Gifts**

Object to Purge	Financial Entities with Purgeable Attachments	Report Data Source
Goods Delivery Abstract	Goods Delivery Runs and Goods Delivery Run Lines	**Goods Delivery Run**
Idea Attachments	Ideas	**Ideas**
Internal Service Delivery	Internal Service Deliveries	**Internal Service Deliveries**
Intraday Bank Statement	Intraday Bank Statements	**Intraday Bank Statements**
Inventory Ship List	Inventory Ship Lists	**Inventory Ship List**
Inventory Stock Request	Inventory Stock Requests	**Inventory Stock Request**
Investment Statement	Investment Statements	**Investment Statements**
Journal Entry	Journal Entries	**Journals**
Miscellaneous Payee	Miscellaneous Payees	**Miscellaneous Payee**
Miscellaneous Payment Request	Miscellaneous Payment Requests	**Miscellaneous Payment Request**
Netting Transaction	Netting Transactions	**Netting Transactions**
OCR Supplier Invoice	OCR Supplier Invoices	**OCR Supplier Invoice** To prevent data corruption, only purge OCR supplier invoices when no Workday supplier invoice was created. For OCR supplier invoices with an associated Workday supplier invoice, purge the supplier invoice document instead.
Period Close	Period Close	**Period Closes**
Procurement Card Transaction Verification	Procurement Card Transaction Verification Headers and Summaries	**Procurement Card Transaction Verifications (Indexed)**
Project Attachments	Projects	**Projects**
Project Event Attachments	Project Events	**Project Events** When you want to purge attachments for a project that wasn't approved, use the Project Events report data source.
Purchase Item Abstract	Purchase Items	**Purchase Items (Indexed)**
Purchase Order	Change Orders, Purchase Orders, and Purchase Order History	**Purchase Orders**
Purchase Order Acknowledgement	Purchase Order Acknowledgements	**Purchase Order Acknowledgments**
Recall	Recalls and Recall Lines	**Recall**

Object to Purge	Financial Entities with Purgeable Attachments	Report Data Source
Recall Response	Recall Responses and Recall Response Lines	**Recall Response**
Receipt	Receipts, Receipt Adjustments, and Receipt Lines	**Receipts**
Recurring Journal Template	Recurring Journal Templates	**Recurring Journal Template**
Recurring Supplier Invoice	Recurring Supplier Invoices	**Recurring Supplier Invoices**
Request for Quote	Request for Quotes and Request for Quotes Lines	**Request for Quotes**
Request for Quote Award	Request for Quote Awards and Request for Quote Award Lines	**Request for Quote Awards**
Request for Quote Response	Request for Quote Responses and Request for Quote Response Lines	**Request for Quote Responses**
Requisition	Requisitions	**Requisitions by Company**
Return to Supplier	Returns to Supplier	**Returns**
Revenue Recognition Schedule	Revenue Recognition Schedule	**Revenue Recognition Schedules**
Signer	Signers	**Signers**
Stop Item	Stop Item	**Stop Items**
Supplier	Suppliers	**View Suppliers Only**
Supplier Contract Abstract	Supplier Contracts, Supplier Contract Amendments, and Supplier Contract History	**Supplier Contract Version** When creating a privacy purge custom report, add the **Supplier Contract Version** report field.
Supplier Invoice Document	Supplier Invoices and Supplier Invoice Adjustments	**Supplier Invoices**
Supplier Invoice Request	Supplier Invoice Requests	**Supplier Invoice Requests**
Supplier Refund	Supplier Refunds	**Supplier Refunds**
Usage Based Transaction Attachments	Usage Based Transaction	**Usage Based Transactions**
Withholding Tax Exemptions	Withholding Tax Exemptions	**Withholding Tax Exemption**

Former Workers

Purgeable Data Type	Description
Audio Pronunciation	Purges audio name pronunciation data.
Contact Information - Contact Information and Related Events	Address: • City. • City - Local.

Purgeable Data Type	Description
	• City Subdivision 1. • City Subdivision 1 - Local. • City Subdivision 2. • City Subdivision 2 - Local. • Comments. • Country. • Country Region. • Lines 1-9. • Lines 1-9 - Local. • Postal Code. • Region Subdivision 1. • Region Subdivision 1 - Local. • Region Subdivision 2. • Region Subdivision 2 - Local. • Validated by Third-Party web service. Instant Messenger: • Address. • Comment. • Type. Email Address: • Address. • Comment. Phone Number: • Area code. • Country code. • Device type. • Extension. • Phone Number. • Usage. Social Network: • Type. • URL. • User name. Web Address: • Comment. • URL.
Names	Local Person Name: • Comment. • First Name. • First Name 2. • Last Name. • Last Name 2. • Middle Name. • Middle Name 2.

Purgeable Data Type	Description
	• Secondary Last Name. • Secondary Last Name 2. All name types: • Comment. • Country (used for name formatting). • First Name. • Full Name. • Last name. • Middle name. • Salutation. • Secondary last name. • Suffix - hereditary. • Suffix - honorary. • Suffix - professional. • Suffix - religious. • Suffix - royal. • Suffix - social. • Title. Preferred Name: • Defer to Legal Name. Additional name: • Additional name type.
Person IDs	Data Purged for these ID types and associated events: • Contingent Worker. • Custom. • Employee. • Former Worker. • Government. • License. • National. • Passport. • Reference ID. • Visa. IDs - All: • Comment. • Expiration date. • ID. • Issued date. • Issuing authority. • Verification date. • Verified by worker. IDs - Custom: • Custom ID type.

Purgeable Data Type	Description
	• Description. • Issued by Organization. IDs - Government: • Government ID type. IDs - License: • License class. • License ID type. IDs - National: • Identifier series. • Issuing Agency. • National ID type. • Issue Date. • Expiration Date. • Issued by. • Comments. IDs - Passport • Issued by country. • Passport ID type.

Personal Information	• Birth city.
	• Birth country.
	• Birth country region.
	• Citizenship status.
	• Comments.
	• Date of death.
	• Disability:
	  • Accommodation provided.
	  • Accommodation requested.
	  • Certification authority.
	  • Certification ID.
	  • Certification location.
	  • Date known.
	  • Degree percent.
	  • End date.
	  • FTE toward quota.
	  • Rehabilitation provided.
	  • Rehabilitation requested.
	  • Remaining capacity percent.
	  • Severity recognition date.
	  • Status date.
	  • Work Restrictions.
	  • Note.
	• Height.

Purgeable Data Type	Description

	• Hukou:
	  • Country region.
	  • Country subregion.
	  • Locality.
	  • Postal code.
	  • Type.
	• Medical exam:
	  • Date.
	  • Expiration date.
	  • Notes.
	• Military:
	  • Discharge date.
	  • Rank.
	  • Service type.
	  • Status.
	• Nationality - Country and country region.
	• Personnel file agency.
	• Photo.
	• Photo comment.
	• Political affiliation.
	• Religion.
	• Social benefits locality.
	• Tobacco use.
	• Weight.

Personal Information - Date of Birth and Age	• Date of Birth.
Personal Information - Ethnicity	• Ethnicity. • Hispanic or Latino. • Ethnicity Visual Survey.
Phonetic Pronunciation	Purges phonetic name pronunciation data.

Previous System History - Job History, Compensation History, Worker Previous System History	Data Purged from Previous System History:
	• Job History.
	  • ID
	• Compensation History.
	  • Compensation Amount Change for Worker History Event
	  • Compensation Amount for Worker History Event
	  • Compensation Previous System History has Currency
	  • Compensation Previous System History has Frequency
	  • ID

Purgeable Data Type	Description

	• Worker History.
	  • Comment
	  • Description for Worker History Event
	  • Effective Date for Worker History Event
	  • Worker History ID
	  • Worker Previous System History for Worker

Reference Letters - Reference Letters, Questionnaires, Uploaded and Generated Documents	Purges: • Questionnaire responses. • Reference letters, including request.
System - System Account Signon	Entire sign-on instance.
System - Username	Username.
Universal ID	Data Purged - Person Universal Identifier.

Job Applications

Purge plans for all job application purgeable data types are optional.

Purgeable Data Type	Description
Activity Stream Comments for Job Application	Purges data related to: • Activity stream comments. • Activity tags. • Activity references. • Notifications.
Candidate and Job Application - Social Share	Purges data related to social share.
Certification Data for Job Application	Purges data related to: • Certification documents. • Certification achievements. • Skills. • Worker documents.
Comments and Notifications for Job Application	Purges data related to: • Comments when you move candidates to different stages. • Notifications initiated by comments or custom notifications. • Notifications initiated by the *Send Message* action. • Workflow notifications.
Education for Job Application	Purges this data: • Degrees • Field of Study • School • First Year Attended • Last Year Attended

Purgeable Data Type	Description
	• Grade Average • Comment • Skills
Experience for Job Application	Purges this data: • Business Title • Job History • Location • Start Month/End Month • Start Year / End Year • Currently Work Here • Total Years of Experience • Years in Current Job • Job Title • Average Year per Job • Responsibilities and Achievements • Skills • Comments
Interview Details for Job Application	Purges data related to: • Interview events. • Attachment comments and files. • Session comments. • Interview notifications and email content. • Questionnaire responses, answers, and attachments. • Comments. • Achievements.
Link Between Person and Job Application	Purges data related to: • Job application EEO information. • Job application merged candidates information. • Agency candidate. • Candidate email. • Emails. • Review Document details such as e-signatures and generated documents. • Employment agreement details.
Personal Information for Job Application	Purges data related to: • Job applications. • Previous worker details. • Resumes.
Personal Reminders for Job Application	Purges this data: • Email content. • Generated documents. • Push notifications. • Notes.

Purgeable Data Type	Description
	• Titles.
Questionnaire Results and Attachments	Purges this data: • Total scores. • Responses. • Answers. • Attachments.
Referral, Endorsement, and Assessment Details for Job Application	Purges data related to: • Emails. • Referred By details. • Endorsements. • Assessments.
Shared Messages	Purges shared messages between workers and related notifications for the job application.
Staffing Event Relationship with Job Application	The link between the job application and staffing event for the job application that you want to purge. Purges the job application event. If a candidate is hired on the job application you want to purge, this purgeable data type removes the link between the job application and the staffing event.

National IDs

Purgeable Data Type	Description
Aadhaar National ID	Purges the 12-digit Aadhaar National ID number.

Payroll

Purgeable Data Type	Applies To	Description
External Payroll Documents	All types of workers.	Purges external payroll documents, including signed or acknowledged copies created through the *Review External Payroll Documents* business process.
Payroll Attachments	• Active workers. • Terminees.	Purges payroll attachments.
Withholding Order Attachments	All types of workers.	Purges withholding order attachments.

Pre-Hires

Workday enables you to purge data for Pre-Hires who don't have a *Candidate*, *Student*, or *Worker* record in Workday. You can purge data for a *Pre-Hire* when:

- The Pre-Hire is created as a standalone Pre-Hire.
- There's no active, terminated, or former *Candidate*, *Student*, or *Worker* record linked to the Pre-Hire.

- The Pre-Hire doesn't have complete or in-progress *Hire* events.
- The Pre-Hire doesn't have incomplete events.

Purgeable Data Type	Description
Contact Information	Purges this data related to Pre-Hire information: • Addresses • Email • Instant Messenger Address • Phone • Web Address
Event Data	Purges activity stream content and comments pertaining to the Pre-Hire.
Names	Purges this data related to the Pre-Hire's Local Person Name: • Comment. • First Name. • First Name 2. • Last Name. • Last Name 2. • Middle Name. • Middle Name 2. • Secondary Last Name. • Secondary Last Name 2. Purges this data related to All Name Types for the Pre-Hire: • Comment. • Country (used for name formatting). • First Name. • Full Name. • Last name. • Middle name. • Salutation. • Secondary last name. • Suffix - hereditary. • Suffix - honorary. • Suffix - professional. • Suffix - religious. • Suffix - royal. • Suffix - social. • Title. Purges this data related to the Pre-Hire's Preferred Name: • Defer to Legal Name. Purges this data related to the Pre-Hire's Additional Name: • Additional name type.

Purgeable Data Type	Description
Person's Payment Elections	Purges this data related to the Pre-Hire's payment elections.
Person's IDs	Purges personal identification data for the Pre-Hire.
Pre-Hire Data	Purges data related to the Pre-Hire in Workday.
Pre-Hire ID	Purges identification data for the Pre-Hire.
Pre-Hire Resume	Purges resume data for the Pre-Hire.
Questionnaire Results	Purges questionnaire answers, scores, and attachments.
System	Purges system instances.
Universal ID	Purges Pre-Hire Universal Identifier.

Questionnaire and Survey Responses

To prevent Workday from adding non-indexed fields as filters when creating a custom report using the *Questionnaire Responses for Purge* **Data Source**, select the **Optimized for Performance** check box. Adding non-indexed fields as filters to your custom report might result in slow performance.

You need to purge Questionnaire and Survey responses independently of purging data for workers. Workday recommends that you purge Questionnaire and Survey responses before purging Worker-related data.

Purgeable Data Type	Purge Person Data Task without Plan	Applies To	Description
Questionnaire and Survey Responses	Required	All	Purges data related to: • Questionnaire Answers. • Questionnaire Attachment. • Questionnaire Responses. • Questionnaire Target. • Questionnaire Target Context. • Survey Answers. • Survey Attachment. • Survey Responses.

Student

Purgeable Data Type	Description
Student Immigration Events	Purges these relationships: • Student Immigration Event residency relationship to Country. • Student Immigration Event relationship to Student Immigration Status.

Purgeable Data Type	Description
	• Student Immigration Event relationship to Student Immigration Status (Metadata).

Student Documents

Purgeable data types for student documents:

- Purge only the document attachments, and not the student.
- Provide retention rules that don't purge:
  - Data for a student with **Do Not Purge** set to True.
  - Financial Aid documents that are less than 3 years from the end of the financial aid award year.
  - Person documents if the person has a role of *Worker*, *Pre-Hire*, or *Candidate* in Workday.

Purgeable Data Type	Report Data Source	Description
Academic Record	**Academic Records**	Purges all transcript order attachments and transcript PDFs related to the student. Includes historical documents for reactivated students.
Education Test Results Documents (Attachments Only)	**Education Test Results**	Purges attachments related to the student's education test results. You can purge attachments from instances of education test results documents by creating a custom report.
External Transcript Documents (Attachments Only)	**Student External Transcript**	Purges attachments related to the student's external transcripts from external education institutions. You can purge attachments from instances of external transcript documents by creating a custom report.
Historical Academic Record	**Historical Academic Records**	Purges all transcript order attachments and transcript PDFs related to the historical student.
Student - Accommodation Documents (Attachments Only)	**Student**	Purges all student document attachments related to accommodations.
Student Application - Action Item Assignments	**Student Application**	Purges documents uploaded to action item assignments for student applications, including: • Attachments, external URLs, and detailed information about the documents. • Action item assignments for duplicate applications that were merged with the applications on the report.

Purgeable Data Type	Report Data Source	Description
Student Application - Documents	**Student Application**	Purges documents uploaded to student applications, including: • Attachments and detailed information about the attachments. • Questionnaire attachments and detailed information about the attachments. • Documents uploaded to duplicate applications that were merged with applications on the report.
Student - Application Documents (Attachments Only)	**Student**	Purges students document attachments related to the student's application.
Student Documents	**Student Documents**	• Includes uploaded Student Documents for accommodations, applications, financial aid, immigration information, residency, and student engagements. • Purges the document attachments and the detail information of the uploaded document.
Student Documents (Attachments Only)	**Student Documents**	• Includes uploaded Student Documents for applications, financials, financial aid, residency, accommodations, and student engagements. • Purges only the document attachments.
Student - Education Test Results Documents (Attachments Only)	**Student**	Purges all education test results attachments related to the student.
Student - External Transcript Documents (Attachments Only)	**Student**	Purges all external transcript attachments for the education institutions related to the student.
Student - Financial Aid Documents (Attachments Only)	**Student**	Purges students document attachments related to the student's completed Financial Aid Action Items. Workday-delivered retention rules only purge Financial Aid documents that are more than 3 years from the Award Year.

Purgeable Data Type	Report Data Source	Description
Student Financials - Direct PLUS Loan Authorization (Attachments Only)	**Student**	Purges students document attachments related to Direct PLUS Loan Authorizations.
Student - International Student Documents (Attachments Only)	**Student**	Purges students document attachments related to international students.
Student Person Documents (Attachments Only)	**Student**	Purges Person Document attachments for a student, except if student also has a role of *Candidate*, *Pre-Hire*, or *Worker*.
Student - Residency Documents (Attachments Only)	**Student**	Purges all student document attachments uploaded for residency.

Student Immigration Data

Purgeable Data Type	Description
Student Immigration Data	Purges this data: • Student Applicant Immigration Event • Student Dependent Immigration Data • Student Immigration Status • Student Immigration Sponsorship Status • Student Documents • Optional Practical Training • External URL

Tax Elections

Purgeable Data Type	Description
Tax Election Form Attachments	Purges tax election form attachments for all types of workers.

Terminees

Purgeable Data Type	Description
Additional Government IDs	• Country. • Government ID Type. • Identification #. • Issue Date. • Expiration Date. • Verification Date. • Verified By.
Benefits - Worker's Dependents, Beneficiaries, Wellness and Tobacco Data	For beneficiaries and dependents (where captured): • City of Birth. • Country of Birth.

Purgeable Data Type	Description

	• Date of Birth.
	• Citizenship Status.
	• Date of Death.
	• Domestic Relations Order.
	• Ethnicity.
	• Gender.
	• Hispanic or Latino.
	• Hukou:
	  • Country.
	  • Country Region.
	  • Country Subregion.
	  • Locality.
	  • Postal Code.
	  • Type.
	• ID.
	• LGBT Identification.
	• Marital Status.
	• Marital Status Date.
	• Medical Exam Date.
	• Medical Exam Expiration Date.
	• Medical Exam Notes.
	• Name.
	• Nationality.
	• Native Country Region.
	• Personnel File Agency.
	• Political Affiliation.
	• Region of Birth.
	• Religion.
	• Social Benefits Locality.
	• Uses Tobacco.
	• Wellness Program Participation.
	• Wellness Score.
	
	Note: Workday identified an issue with the Purge Person Data process where we successfully purged data on the beneficiary object, but beneficiary details remained on the Change Beneficiary event. We resolved this issue as of May 19, 2018. For Purge Person Data tasks completed before May 19, 2018, which include beneficiaries to be purged along with the person data for Terminated Workers, rerun the purge task against your purge custom reports. The purge shall then successfully execute on the remaining beneficiary details.
	
	For workers:
	
	• Uses Tobacco.
	• Wellness Program participation.
	• Wellness Score.

Purgeable Data Type	Description
	Also, attachments and worker documents for all events where the worker's dependent or beneficiary is the subject.
Compensation - Additional Compensation Data includes Allowances, Base Pay, Commission, Stock and Bonuses	Enables you to purge compensation-related data from the employee and from the associated launched events. The amounts will no longer be available when reporting on the overall process. Example: When using the report data source Merit Process Employee Adjustments. Data purged: • Ad Hoc Compensation. • Bonus Plan. • Compensation Payment. • Eligible Earnings Overrides. • Future Payment Plan. • Guidelines. • One-Time Payments. • Period Activity. • Period Activity Eligibility. • Plan Assignment. • Proposed Compensation Package Assignments. • Severance Worksheet. • Severance Package Component. • Statutory Compensation Statement. • Step. • Stock Grant Event - stock plan and stock grant.
Compensation - Core	Purges attachments for terminated workers on these business processes: • Change Default Compensation. • One-Time Payment for Referral. • Period Activity Pay. • Propose Compensation Change. • Propose Compensation Hire. • Propose Compensation Offer/Employment Agreement. • Request Compensation Change. • Request Compensation Change for Leave of Absence. • Request One-Time Payment. • Request One-Time Payment for Self. • Request One-Time Payment Offer/Employment Agreement. • Request Stock Grant.
Compensation - Merit Statements, and Merit, Bonus and Stock Notes	Enables you to continue to report on the compensation adjustment amounts, but the amounts are no longer associated with the worker. Example: The amount is still available

Purgeable Data Type	Description
	when reporting from the report data source All Compensation Review Employee Adjustments. Workday purges data that is particular to the employee, including comments for: • One Time Payments. • Pay Adjustments (merit and bonus). • Stock Plan Awards. Also, documents generated as business forms. Example: Merit Statements.
Contact Information - Contact Information and Related Events	Address: • City. • City - Local. • City Subdivision 1. • City Subdivision 1 - Local. • City Subdivision 2. • City Subdivision 2 - Local. • Comments. • Country. • Country Region. • Lines 1-9. • Lines 1-9 - Local. • Postal Code. • Region Subdivision 1. • Region Subdivision 1 - Local. • Region Subdivision 2. • Region Subdivision 2 - Local. • Validated by Third Party web service. Instant Messenger: • Address. • Comment. • Type. Email Address: • Address. • Comment. Phone Number: • Area code. • Country code. • Device type. • Extension. • Phone Number. • Usage. Social Network: • Type. • URL. • User name.

Purgeable Data Type	Description
	Web Address: • Comment. • URL.
Event Data - Comments, Uploaded Documents, Attachments, and Delivered Reports	• Attachments and worker documents for all events where the worker is the subject, as well as comments for those attachments and documents. • Activity Stream content and comments pertaining to the Worker.
Financials - Expense Reports	• Attachments (include uploaded images). • Line Memo. • Memo (overall).
Financials - Procurement Card Transactions	• Attachments and attachment comments. • Memos (document, line and line split).
Financials - Worker Credit Card	• Cardholder embossed name. • Description.
Form I-9 - Exceeding the Retention Requirements	2013 and later revisions of the Form I-9, initiated between March 2013 and the present: • All Form I-9 data – optional. Applies to Form I-9s on the purged worker surpassing the USCIS retention requirements (3 years after the first day of employment or 1 year after termination). If you purge Person data but don't decide to purge Form I-9 data, or we didn't purge a Form I-9 due to retention requirements, you can purge the Form I-9 later when the retention requirement passes. 2009 revision of the Form I-9, initiated approximately between March 2012 and March 2013: • Employee data and document data – not optional. Includes Employee Legal Name, Employee Home Address, Maiden Name, Social Security Number, Date of Birth, and List A, B, and C document details, when completed. • Remaining data – optional. If you want to purge the remaining data on a 2009 Form I-9, you must select the Form I-9 area. This purge is subject to the retention requirements. **Note:** If you want to purge person data for a worker who has a 2009 revision Form I-9 and

Purgeable Data Type	Description
	don't want to purge Form I-9 data, open a case with Workday support.
Licenses	• License ID Type. • Class Issued by Country / Issued by Country Region / Issued by Authority. • Identification #. • Issued Date. • Expiration Date. • Verification Date. • Verified By.
Names	Local Person Name: • Comment. • First Name. • First Name 2. • Last Name. • Last Name 2. • Middle Name. • Middle Name 2. • Secondary Last Name. • Secondary Last Name 2. All name types: • Comment. • Country (used for name formatting). • First Name. • Full Name. • Last name. • Middle name. • Salutation. • Secondary last name. • Suffix - hereditary. • Suffix - honorary. • Suffix - professional. • Suffix - religious. • Suffix - royal. • Suffix - social. • Title. Preferred Name: • Defer to Legal Name. Additional name: • Additional name type.
Other Global - Contract, Collective Agreement, Worker Documents	Collective agreement: • Factors and factor options. Employee Contract:

Purgeable Data Type	Description
	• Description. • Date Signed - Employee. • Date Signed - Employer. • End Date. • ID. • Start Date. • Version Date. Worker documents: • Worker documents. • Supporting documents (Example: certifications), for workers, dependents, and beneficiaries, as well as comments on these documents.
Other IDs	• Other ID Type. • Organization. • Description. • Identification #. • Issued Date. • Expiration Date
Passports	• Country. • Passport ID Type. • Identification #. • Issued Date. • Expiration Date. • Verification Date. • Verified By.
Payroll - External Payroll Data	External Payslip: • Comments. • Related attachment. External Tax Document: • Comments. • Related attachment.
Payroll - Payment Elections Data	• Payment election enrollment and associated event.
Person IDs	Data Purged for these ID types and associated events: • Contingent Worker. • Custom. • Employee. • Former Worker. • Government. • License. • National. • Passport.

Purgeable Data Type	Description
	• Reference ID. • Visa. IDs - All: • Comment. • Expiration date. • ID. • Issued date. • Issuing authority. • Verification date. • Verified by worker. IDs - Custom: • Custom ID type. • Description. • Issued by Organization. IDs - Government: • Government ID type. IDs - License: • License class. • License ID type. IDs - National: • Identifier series. • Issuing Agency. • National ID type. • Issue Date. • Expiration Date. • Issued by. • Comments. IDs - Passport • Issued by country. • Passport ID type.
Person Shared Addresses with Location - Address data for Worker and for Worker's Dependents, Beneficiaries, and Emergency Contacts that is shared with a Location	Purges a worker's address and the worker's related persons' addresses that are shared with a Location. The Location address won't be purged; only disconnected from the worker and/or related persons.
Personal Information	• Birth city. • Birth country. • Birth country region. • Citizenship status. • Comments. • Date of death.

Purgeable Data Type	Description

	• Disability:
	  • Accommodation provided.
	  • Accommodation requested.
	  • Certification authority.
	  • Certification ID.
	  • Certification location.
	  • Date known.
	  • Degree percent.
	  • End date.
	  • FTE toward quota.
	  • Rehabilitation provided.
	  • Rehabilitation requested.
	  • Remaining capacity percent.
	  • Severity recognition date.
	  • Status date.
	  • Work Restrictions.
	  • Note.
	• Height.
	• Hukou:
	  • Country region.
	  • Country subregion.
	  • Locality.
	  • Postal code.
	  • Type.
	• Medical exam:
	  • Date.
	  • Expiration date.
	  • Notes.
	• Military:
	  • Discharge date.
	  • Rank.
	  • Service type.
	  • Status.
	• Nationality - Country and country region.
	• Personnel file agency.
	• Photo.
	• Photo comment.
	• Political affiliation.
	• Religion.
	• Social benefits locality.
	• Tobacco use.
	• Weight.

Personal Information - Date of Birth and Age	• Date of Birth.
Personal Information - Ethnicity	• Ethnicity. • Hispanic or Latino.

Purgeable Data Type	Description
	• Ethnicity Visual Survey.
Personal Information - Gender	• Gender.
Personal Information - Marital Status	• Marital Status. • Marital Status Date.
Personal Information: Country Specific Section 1	Purges: • Country Specific Section 1 - Field 1 • Country Specific Section 1 - Field 2 • Country Specific Section 1 - Field 3
Personal Information: Country Specific Section 2	Purges: • Country Specific Section 2 - Field 1 • Country Specific Section 2 - Field 2 • Country Specific Section 2 - Field 3
Personal Information: Country Specific Section 3	Purges: • Country Specific Section 3 - Field 1 • Country Specific Section 3 - Field 2 • Country Specific Section 3 - Field 3
Personal Information: Non Country Specific Section 1	Purges: • Non Country Specific Section 1 - Field 1 • Non Country Specific Section 1 - Field 2 • Non Country Specific Section 1 - Field 3
Personal Information: Non Country Specific Section 2	Purges: • Non Country Specific Section 2 - Field 1 • Non Country Specific Section 2 - Field 2 • Non Country Specific Section 2 - Field 3
Personal Information: Non Country Specific Section 3	Purges: • Non Country Specific Section 3 - Field 1 • Non Country Specific Section 3 - Field 2 • Non Country Specific Section 3 - Field 3
Previous System History - Job History, Compensation History, Worker Previous System History	Data Purged from Previous System History: • Compensation History. • Job History. • Worker History.
Recruiting Agency User Documents (Attachments Only)	Purges all recruiting agency user document attachments.
Reference Letters - Reference Letters, Questionnaires, Uploaded and Generated Documents	Purges: • Questionnaire responses. • Reference letters, including request.

Purgeable Data Type	Description

Related Persons - Personal Information for Dependents, Beneficiaries and Emergency Contact	For dependents, beneficiaries, and emergency contacts:
	Address:
	• City.
	• City - Local.
	• City Subdivision 1.
	• City Subdivision 1 - Local.
	• City Subdivision 2.
	• City Subdivision 2 - Local.
	• Comments.
	• Country.
	• Country Region.
	• Lines 1-9.
	• Lines 1-9 - Local.
	• Postal Code.
	• Region Subdivision 1.
	• Region Subdivision 1 - Local.
	• Region Subdivision 2.
	• Region Subdivision 2 - Local.
	Note: If you purge the Related Persons purgeable data type and a worker shares their address with a dependent, beneficiary, or emergency contact, Workday also purges the address of the worker.
	Demographic/Biographic:
	• Birth city.
	• Birth country.
	• Birth country region.
	• Birthdate.
	• Citizenship status.
	• Date of death.
	• Ethnicity.
	• Gender.
	• Height.
	• Hukou:
	  • Country region.
	  • Country subregion.
	  • Locality.
	  • Postal code.
	  • Type.
	• LGBT identification.
	• Marital status.
	• Marital status date.
	• Medical exam date.
	• Medical exam expiration date.
	• Medical exam note.
	• Military discharge date.
	• Nationality.

Purgeable Data Type	Description
	• Native country region. • Personnel file agency. • Political affiliation. • Religion. • Social benefits locality. • Tobacco use. • Validated by third-party web service. • Weight. Comments - all forms of contact. Email: • Address. Emergency contact: • Preferred language. • Relationship to worker. IDs - All: • Expiration date. • ID. • Issuing authority. • Verified by worker. IDs - Custom: • Description. • Issued by organization. • Issued date. • Type. • Verification date. IDs - Government: • Government ID type. IDs - License: • License ID type. IDs - National: • National ID type. • National ID series. IDs - Passport: • Passport ID type. IDs - Visa: • Visa ID type. Instant messenger: • Address. • Type. Name (all): • Country for name formatting.

Purgeable Data Type	Description
	• First Name. • Full Name. • Last name. • Middle name. • Salutation. • Secondary last name. • Suffix - academic. • Suffix - hereditary. • Suffix - honorary. • Suffix - professional. • Suffix - religious. • Suffix - royal. • Suffix - social. • Title. Name - local: • First name. • First name 2. • Last name. • Last name 2. • Middle name. • Middle name 2. • Secondary last name. • Secondary last name 2. Name - preferred: • Defer to legal name. Phone: • Area code. • Country code. • Device type. • Extension. • Phone number. • Usage. Social network account: • URL. • User name. • Web address.
Self-Identification - Sexual Orientation, Gender Identity, Pronoun	Purges: • Sexual Orientation and Gender Identity. • Sexual Orientation. • Gender Identity. • Pronoun.
Social Network Accounts	• Facebook. • Google+. • LinkedIn.

Purgeable Data Type	Description
	• Twitter.
System - System Account Signon	• Entire sign-on instance.
System - Username	• Username.
Talent - Worker's Performance, Goal and Skill Data	Accomplishment: • Completion date. • Description. • Start date. • While in position. Assessment: • Achievable level. • Loss impact. • Nomination. • Notes. • Potential. • Potential assessment review rating. • Retention. • Talent matrix placement review rating. Award: • Awarding body. • Date received. • Description. • Name. Career preferences: • Goals. • Responsibility. Certification: • Country. • Examination date. • Examination score. • Expiration date. • Issued date. • Issuer. • Name. • Number. • Speciality achievement. Competency: • Assessment comment. Development item: • Additional information. • Removed. • Status. • Status note.

Purgeable Data Type	Description

	• Tag.
	• Title.
	Education:
	• Attended:
	  • First day.
	  • First year.
	  • Last day.
	  • Last year.
	• Country.
	• Date degree received.
	• Degree.
	• Field of study.
	• Grade average.
	• Institution.
	• Institution location.
	• School.
	• School type.
	Feedback given:
	• About worker.
	• Response.
	Feedback requested:
	• Confidential.
	• Question:
	  • Question.
	  • Tag.
	• Response:
	  • Comment.
	  • Declined.
	  • Declined reason.
	  • Praise.
	  • Tag.
	• Responder.
	Goal:
	• Cascaded from goal.
	• Goal note.
	• Goal note deleted.
	• Milestone:
	  • Detail.
	  • Due date.
	  • Name.
	  • Removed.
	  • Status.
	Job interest:
	• Note.

Purgeable Data Type	Description
	• Work assignment. Job history: • Business title. • Company. • Contact information. • End date. • Location. • Reference. • Responsibilities and achievements. • Start date. Job interest: • Job profile. Internal project experience: • Description. • End date. • Leader. • Name. • Start date. Language: • Ability. • Assessment comment. • Language. • Native language. • Preferred language. Membership: • Affiliation. • Affiliation relationship type. • Organization. • Member since. Relocation preferences: • Additional information. • Long-term relocation area. • Short-term relocation area. • Willing to relocate - long term. • Willing to relocate - short term. Succession plan candidate: • Notes. • Plan. • Readiness. Succession pool candidate: • Note. • Pool. • Readiness.

Purgeable Data Type	Description

	• Top candidate.
	Talent review:
	• Additional reviewer type.
	• Calibrated review rating.
	• Component completion.
	• Employee summary.
	• Evaluation comment.
	• Manager evaluation:
	  • Comment - employee.
	  • Comment - manager.
	  • Status.
	  • Summary.
	• Overall rating.
	• Period start date.
	• Period end date.
	• Rating override.
	• Review content.
	• Review section.
	• Section calculated rating.
	• Section rating override.
	• Summary details.
	• Worker goal:
	  • Category.
	  • Completion date.
	  • Description.
	  • Detail weight.
	  • Due date.
	  • Name.
	  • Proposed by worker.
	  • Removed.
	  • Status.
	  • Superior organization goal.
	Training:
	• Completion date.
	• Description.
	• Program name.
	• Type.
	Travel preferences:
	• Additional information.
	• Amount.
	• Mobility choice.
	Work experience:
	• Comment.
	• Work experience.

Purgeable Data Type	Description
	Also, documents generated as business forms. Example: Talent cards.
Time Tracking - Comments for Worker's Time Blocks	• Time block comments.
Union Membership	Purges: • Comments. • Member of Union. • Membership end date. • Membership start date. • Seniority Date. • Union Seniority Date. • Union Type.
Universal ID	Data Purged - Person Universal Identifier.
Visas	• Country. • Visa ID Type. • Identification #. • Issued Date. • Expiration Date. • Verification Date. • Verified By.
Worker ID	• Employee ID.

Related Information
Reference
2023R2 What's New Post: Purgeable Data Types

FAQ: Purge Person Data

Why can't I purge some data?

The data purge report includes a list of *People with Data that Could Not Be Purged*. To purge a worker's data, without a plan or with a Terminated PII (Workday Owned) plan, that worker must meet all of these criteria:

- Have no other active statuses such as Retiree, Candidate, Academic Affiliate, or Student (or future events to make them such).
- Have no outstanding compensation or benefits events.
- Have no incomplete payroll or retro pay results.

For certain data, the worker must also be a terminated worker before the data is available for purging.

For absence data, you can purge data for terminated workers only for these data types:

- Absence Case Events for Worker.
- Absence Occurrence.
- Worker's Absence Balance Components.
- Worker's Leave of Absence Events.
- Worker's Time Off Events.

For active workers, you can only purge data for the Worker's Absence Comments and Attachments data type.

To ensure accurate payroll records, Workday requires a waiting period before deleting a former employee's absence data. You can only purge this data after these timeframes have passed since their termination date:

- UK: 6 years
- France: 5 years
- USA: 3 years
- Canada: 7 years

Workday applies the data purging validation by comparing the location for the worker's position on their last termination event to the list of payroll enabled countries in the tenant setup.

Can I purge data for active workers?

Yes. There are data types that are purgeable for active workers. You can process terminated workers or active workers in a given run of **Purge Person Data**.

If a terminated worker is also a candidate, is the candidate data purged?

Yes. The task purges all personally identifiable information (PII).

Are terminated workers, who still receive compensation or benefits, included in purges?

No. If a terminated worker is still receiving any form of compensation or has an active benefit plan, Workday doesn’t purge the terminated worker.

What if we’re required to keep financial data for a longer period of time?

You can set the **Years to Retain Financial Data for Purged Workers** on the **Edit Tenant Setup - Financials** task. Workday preserves the financial data regardless of the privacy purge parameters.

Related Information
Reference
The Next Level: Data Purging

FAQ: Reporting on Purged Persons

Do reports display purged workers?

Workday displays purged workers with the name *Purged Person*, and they continue to be displayed in processes where they were participants. Example: Workday displays a terminated and purged manager *Purged Person* in employee reviews.

Authorized users can view the details of purged workers through the worker profile. Workday removes any purged data from the worker profile, and retains references to corporate data such as organizations and job profiles.

Do integrations display purged workers?

If the integration includes terminated workers, and those workers have been purged, Workday returns them in reports. However, the reports won't include any purged data associated with the terminated workers.

If the integration doesn't include terminated workers, it might still return purged workers. To exclude purged workers from the report output, filter on the **Person Purged** field.

How to exclude purged workers from returning in reports?

You can exclude persons by setting the field **Person Purged** to *No*. Workday secures the field to these domains in the Staffing functional area:

- Worker Data: Active and Terminated Workers.
- Worker Data: Terminations

How to include custom reports in the population to purge?

In order for a custom report to display in the **Population to Purge** prompt, the report must:

- Be tagged with **Purge**.
- Be written from a report data source that is based on the **Worker** business object.
- Have no run-time prompts.
- Meet other requirements for the Alert Notification framework.

The person running the **Purge Person Data** task must have unconstrained access to all the resulting rows and columns that report could return.

For **Former Workers** only, in the **Prompt** tab, under **Prompt Defaults**, add these fields, and select **Do Not Prompt at Runtime**:

- **Worker Type**.
- **Termination Date From**.
- **Termination Date To**.

Related Information
Reference
The Next Level: Data Purging

Concept: Purging Person Privacy Data

Data protection laws might require you to delete personal data from the tenant when you no longer need it. Workday enables you to purge specified Personally Identifiable Information (PII).

When you purge data, you permanently remove it from your tenant. Workday can't reverse a data purge.

Only grant the ability to purge data to users who understand the purging process and its consequences. Typically, security administrators perform data purges.

The Data Purging Process

Workday purges specific PII for the population you identify in a custom report. Example: You can define a report to purge job application data for specific workers.

Note: Workday can’t reverse or roll back the deletion. Always test the custom report and purge in your Sandbox environment before you purge any data in your Production environment.

Workday only purges workers who are:

- Marked as eligible for purge in the custom report.
- Terminated. The worker can't have another active worker position or a pending termination.

Workday doesn’t purge workers who are:

- Retirees.
- Academic affiliates. Example: Admissions counselor.
- Students.
- Candidates for an open or frozen job.
- Future hires.

The worker can't have any outstanding payroll, compensation, or benefit events, such as:

- Incomplete payroll.
- Retro payroll.
- Compensation reviews.

Purge Plans

Workday enables you to create and manage purge plans for use with the **Purge Person Data** task. Purge plans enable you to preselect specific types of PII to include in the purge. You can use these plans when you periodically need to purge well-defined sets of user data (Example: For terminated workers). Workday also supplies purge plans.

When you run the **Purge Person Data** task with your own purge plan, Workday purges only the PII that you specify in the plan. Workday doesn't indicate instances as **Purged Person**, and doesn't identify them as completely purged. Example: When you purge name data using your own purge plan, Workday purges (nulls) the names, although other PII might remain.

Workday doesn't enable creating or editing external I-9 forms for purged workers, because it filters out purged workers. However, when you use your own purge plan to do a partial purge, you can still create or edit external I-9 forms for the partially purged workers.

Purging Workers

When you purge workers, Workday no longer returns them in searches, and Workday removes all PII. For historical headcount purposes, they remain in Workday with the name of **Purged Person**.

Integrations returning terminated workers include purged persons, but doesn’t include any purged data.

Purging Terminated Worker Data

Workday provides a *Terminated PII (Workday Owned)* purge plan. When you run the **Purge Person Data** task with that purge plan, Workday performs these actions for each person in your custom report:

- Purges the set of data that Workday automatically selects for mandatory deletion.
- Purges attachments and comments on any remaining data associated with the purged person.
- Indicates the instance as **Purged Person** wherever their name normally displays.
- Associates any remaining data with **Purged Person** instead of an identifiable person.

To purge the dependents and beneficiaries of a terminated worker, you must purge the worker.

You can also run the **Purge Person Data** task for terminated workers without a purge plan. Doing so produces the same result as when you use the *Terminated PII (Workday Owned)* purge plan. You can also select to purge additional PII.

Privacy Purge

In a **Privacy Purge**, Workday doesn't delete objects, but instead removes PII and preserves referential integrity. Example: Logan McNeil wrote a review for Bob Smith, and you purge Logan. The review then displays that **Purged Person** wrote it.

Confirming Data Has Been Purged

Create a report that displays the population and the data that is purgeable. Then run it before and after the purge for comparison.

Excluding Workers from Data Purge

You need to identify people in a way that enables you to include them in your custom report filter. Otherwise, you can build a custom organization and assign the people individually. When you construct your report, make sure that your filter criteria excludes that talent pool or organization.

Purging Data for a Specific Person

Create a custom report that selects the specific person. Run that report within the **Purge Person Data** task and select the appropriate data types.

Defining Purging Responsibilities by Country

To limit purging responsibilities by country:

1. Separate the users who can run **Purge Person Data** by specific country:
   a. Create User-based Security Groups by country and assign only people authorized to purge data by specific country. Example: *Purge Users: France*, *Purge Users: Germany*.
   b. Create an Aggregate Security Group to be used with the **Purge Person Data** domain and add the specific country security groups to it.
2. Create custom reports by country and share the report with the security group that's specific to that country.

Related Information
Tasks
Create a Privacy Purge Custom Report on page 285
Reference
Reference: Purgeable Data Types on page 287
The Next Level: Data Purging

Data Scrambling

Setup Considerations: Data Scrambling

You can use this topic to help make decisions when planning your configuration and using data scrambling in your Implementation tenants for training and testing. It explains:

- Why to set it up.
- How it fits into the rest of Workday.
- Downstream impacts and cross-product interactions.
- Security requirements and business process configurations.
- Questions and limitations to consider before implementation.

Refer to detailed task instructions for full configuration details.

What It Is

With Workday, you can use data scrambling to replace sensitive worker data with irreversibly scrambled data in your Implementation tenants.

Business Benefits

Data scrambling limits exposure to personal or sensitive identifiable information, enabling you to test new features and train your personnel.

Use Cases

You need to:

- Demonstrate a new feature that you want workers to adopt, but need to protect personal and sensitive information.
- Create training materials on how to fill out documents, but generating custom data is too time-consuming.

- Test a new feature, or perform regression testing on an existing feature, but need to protect personal and sensitive information.

Questions to Consider

Questions	Considerations
What fields should you scramble?	Consider how you use your tenant to help you decide which fields to scramble. Example: You want to scramble National ID data to test a business process for hiring a worker. However, scrambling National ID data might not make sense for testing an integration for payroll.
What happens when you scramble username data? How can you identify other users after you scramble usernames?	When you create a scramble plan that includes usernames, Workday scrambles all username data except for the username of the user that runs the task to generate data scramble values. You must: • Identify users who need access to the tenant. • Provide those users with their scrambled usernames to sign in to the tenant. You can identify users by fields that you didn't scramble (Example: Employee ID), or by their position in the organization chart.
How long does it take to scramble data?	Data scrambling aims to take less than 24 hours to complete. However, the scramble time depends on the number of: • Attributes you select to scramble. • Data entries for those attributes. • Compensation fields you select to scramble. These items could cause data scrambling to take longer than 24 hours to complete. Once you initially scramble a tenant, selecting only to regenerate values that have changed since you last generated them might reduce the time to rescramble the tenant.
What does scrambled data look like?	Workday uses different scramble methods. Example: Workday alternates between random consonants and vowels when scrambling first names.
What tenants can you scramble your data in?	You can only scramble data in your Implementation tenant.
When you access data through an API, does the API return scrambled data?	Yes, based on the fields you selected for your scramble plan, the API accesses scrambled data for those fields. However, if you have integration files that existed before scrambling, the files won't contain scrambled data.

Recommendations

Limit the number of people who can access to the *Scramble Administration* domain. Limiting access prevents others from accidentally scrambling the tenant without proper communication or training.

Create the scramble plan in your Production tenant so you can repeatedly scramble based on the original plan. You can create scramble plans in your Implementation tenant. You'll have to recreate those plans, however, when the tenant refreshes from production.

Back up your Implementation tenant and integration files before beginning the data scramble value generation process. You can revert the data from your backup if:

- There's data you didn't intend on scrambling.
- The data didn't scramble the way you expected.

Access the **Manage Workday Maintenance Window** task to notify users before running these tasks:

- **Generate Scramble Values**
- **Start Data Scramble**

If you access the **Generate Scramble Values** task, the tenant might not perform as quickly for other users. For the **Start Data Scramble** task, the tenant is unavailable for other users.

Run the **Generate Scramble Values** and the **Start Data Scramble** tasks with plenty of time before the Weekly Service Update. Otherwise, the tenant won't have scrambled data after the Weekly Service Update.

Requirements

No impacts.

Limitations

You can only scramble data in your Implementation tenant.

When generating data scramble values, Workday might not scramble the data that users enter while the task is running.

Data scrambling doesn't guarantee scrambling every instance in a tenant. It also doesn’t prevent everyone using the implementation tenant from viewing specific data or identifying a worker from scrambled data.

Once you scramble values in your tenant, the scrambled data is irreversible.

Tenant Setup

No impacts.

Security

Users secured to the *Scrambler Administration* domain in the System functional area can:

- Create scramble plans.
- Generate data scramble values.
- Start data scrambling.

Users secured to the *Scrambler Administration* domain are exempt from having their data scrambled.

Business Processes

No impacts.

Reporting

Reports	Considerations
View Data Scramble Plan	Use this report to verify all fields that you intend to scramble.
View Data Scramble Status	Use this report to view the status of data scramble value generation and scrambling operations for the data scramble plans in the tenant.
View Data Scrambling Plan Status History	Use this report to view the complete history of the scrambling status for a data scramble plan.

Integrations

Verify the downstream impacts of data scrambling if you use an integration. Example: If you use a payroll integration or have a Benefits vendor, they might need access to unscrambled personal data.

Connections and Touchpoints

Data scrambling interacts with these products in Workday:

- Compensation.
- Compliance.
- Expense.
- Payroll.
- Staffing.
- Student.
- Talent.
- Worker Information.

The data you decide to scramble determines the touchpoints.

Workday offers a Touchpoints Kit with resources to help you understand configuration relationships in your tenant. Learn more about the Workday Touchpoints Kit on Workday Community.

Related Information
Reference
The Next Level: Data Scrambler
Workday Community: Refresh Tenant Request

Steps: Scramble Tenant Data

Prerequisites

Review Concept: Data Scrambling on page 339.

Context

You can create and run scramble plans to replace, permanently and irreversibly, original data with scrambled data in your implementation tenant. Workday enables you to create 1 or more scramble plans that include selected fields and scramble methods. Example: You can create separate scramble plans for training and testing. When you run the scramble plan in your implementation tenant, Workday generates scrambled data values for the selected fields based on the scramble methods.

Workday recommends that you create your data scrambling plan in your production tenant. Workday copies the scramble plan to your implementation tenant during the tenant refresh. You can also create

scramble plans in your implementation tenant; however, Workday overwrites them during the tenant refresh.

Note: If you include **User Name** in your scramble plan, Workday scrambles all usernames in the tenant except for the username of the user who runs the **Generate Data Scramble Values** task. After scrambling data, you need to:

- Identify users who need access to the tenant.
- To enable users to sign into the tenant, provide those users with their scrambled usernames or new usernames.

You can identify users by fields that you didn't scramble (Example: Employee ID), or by their position in the organization chart.

You can run the **View Data Scramble Status** report anytime to check the status of the data scramble value generation and data scrambling processes.

Steps

1. Edit Domain Security Policies on page 200.

   In your production and implementation tenants, grant **View** and **Modify** access to the *Scrambler Administration* domain for security groups to enable them for data scrambling. The *Scrambler Administration* domain is in the System functional area. Usernames secured to this domain are exempt from having their data scrambled.
2. Activate Pending Security Policy Changes on page 203.

   Activate the security policy changes in both tenants.
3. In your production tenant, access the **Create Data Scramble Plan** task.

   As you complete the task, consider:

Option	Description
Select All Fields	Includes all available scramble fields in all areas to your plan.
Select All Area Fields	Includes all available scramble fields in the area to your plan.
Scramble Method	Select how Workday scrambles data. Example: You can scramble the **First Name** field to display as a string of alternating consonants and vowels.

   Security: *Scrambler Administration* domain in the System functional area.
4. Access the **View Data Scramble Plan** report.

   You can review the report to verify that you selected only fields that you want Workday to scramble and the scramble methods.

   You can also export the report and review it offline.

   Security: *Scrambler Administration* domain in the System functional area.
5. To have Workday refresh your implementation tenant from your production tenant, submit a refresh tenant request in the Workday Customer Center.

   Only your Named Support Contact can submit the refresh tenant request.
6. In the implementation tenant, access the **Generate Data Scramble Values** task.

   The first time you run the **Generate Data Scramble Values** task for your scramble plan, Workday maps all field values in the scramble plan to scrambled values in the tenant. If you regenerate data scramble

values using the same plan, selecting **Scramble modified values** preserves the scrambled values for fields that haven't changed in the plan.

The mapping process starts immediately if you don't set a **Schedule**. You can schedule the **Generate Data Scramble Values** task to run only once at a future date and time. Workday sends a notification when the mapping process completes. If the data scramble value generation doesn't complete, you might need to rerun the task.

Workday limits the number of generated scramble values that it stores in the tenant to 10. If you receive an error when running the **Generate Data Scramble Values** task, access the **Delete Generated Scramble Values** task. You can delete scramble values for previously stored data scramble plans with that task.

Security: *Scrambler Administration* domain in the System functional area.

7. In the implementation tenant, access the **Start Data Scramble** task.

   As you complete the task, consider:

Option	Description
Restart Tenant and Scramble Values Immediately	All users immediately lose access to the implementation tenant, which remains unavailable until the tenant restart completes.
Scramble Values During Next Planned Weekly Service Update or Tenant Restart	Workday scrambles the data when the next tenant restart occurs, or during the weekly service update. If you select this option and then want to cancel the data scrambling operation, you can access the **Stop Data Scramble** task. Run the **Stop Data Scramble** task before the next tenant restart or weekly service update.

   Security: *Scrambler Administration* domain in the System functional area.

Result

You can view the scrambled field values in the implementation tenant only after the **Start Data Scramble** task completes and the tenant restarts.

Next Steps

Carefully review the tenant after scrambling to determine whether the results meet your requirements. You can edit your plan to add or remove fields and then scramble the data again.

Related Information
Concepts
Workday Community: Refresh Tenant Request

Concept: Data Scrambling

Workday enables you to permanently and irreversibly scramble original data in implementation tenants for training and testing. Data scrambling:

- Alters the original field values so that users won't be able to derive them from the scrambled data.
- Maintains the overall structure of your organization data.

Note: Data scrambling isn't anonymization and using this feature doesn't exempt you from applicable data privacy laws. Workday recommends that you exercise caution when scrambling implementation tenant data. Data scrambling is irreversible. It's important that you understand the impact of the selected fields and methods when setting up your data scrambling plan. Data scrambling can remove access to existing

documents in your implementation tenant. If you scramble names or user names, Workday displays past transactions as run by the scrambled names or user names.

Scope of Data Scrambling

The **Data Scrambling** task scrambles data objects; it doesn't look at person types. Example: If you scramble a data object that Workday reuses across person types, then Workday scrambles the data object only for those roles.

Data scrambling doesn't scramble every instance of a field. It also doesn't prevent anyone viewing the implementation tenant from seeing specific data or identifying a worker from scrambled data. Data still exists in the tenant that Workday doesn't scramble.

Data scrambling doesn’t scramble all personal information in the tenant. Example: Scrambling worker name fields won’t scramble all instances of the names in your implementation tenant, such as worker names in comments. Carefully review the tenant after scrambling to determine whether the results meet your requirements. Examples: You might:

- Review organization charts to verify scrambled values for worker names.
- Test business processes or custom reports to verify scrambled values for date of birth.

How Data Scrambling Works

Data scrambling enables you to scramble selected fields in your implementation tenant using a data scramble plan you create in your production tenant. When the implementation tenant refresh occurs, Workday copies the scramble plan from your production tenant, and then you can use the plan to scramble data in selected fields.

The data scrambling process involves these tasks:

- The **Create Data Scramble Plan** task enables you to select fields you want to scramble, and the methods by which you want to scramble them.
- The **Generate Data Scramble Values** task maps unscrambled field values to their scrambled values in the tenant. Workday doesn't scramble the tenant data when you run the **Generate Data Scramble Values** task.
- When you run the **Start Data Scramble** task, Workday replaces field values with scrambled values in the tenant using the mapping. Workday scrambles the tenant data after you run the **Start Data Scramble** task.
- The **View Data Scramble Status** report displays the status of data scramble value generation and scrambling operations for each data scramble plan.

Workday provides 2 options when you run the **Generate Data Scramble Values** task:

- **Scramble all values** - When you select this option, Workday generates new scrambled values for all of the fields in the selected scramble plan. This option rescrambles user name data if you've included in your plan. You'll therefore need to provide users with their scrambled user names again so that they can sign in to the tenant.
- **Scramble modified values** - When you select this option, Workday only generates new scrambled values for fields in the selected scramble plan that are new or have changed since you last ran the **Generate Data Scramble Values** task. Select this option if you want to preserve scramble values that haven't changed in your scramble plan.

The **Start Data Scramble** task has options that enable you to either:

- Start the data scrambling process immediately.
- Wait until the next tenant restart or weekly service update.

If you start the data scrambling process immediately, all users lose access to the implementation tenant immediately. The tenant then remains unavailable until the tenant restart completes.

Schedule Considerations

The Data Scrambling process can take over 24 hours to complete. We recommend that you plan your scrambling schedule to accommodate this timeframe. Example: For an implementation tenant containing 1 million workers:

- The **Generate Data Scramble Values** task can take up to 24 hours to complete.
- The **Start Data Scramble** task can take an additional 2 hours to complete. Once the task completes and the tenant restarts, Workday indexes the scrambled values, which can take over 24 hours to complete. Until indexing completes, you might find missing or incomplete search results in the tenant.

Other factors to consider are:

- Daily Tenant - maintenance request deadline.
- Implementation Tenant - maintenance window you select.
- The quantity of data in the source tenant.

Other Considerations

Workday might not scramble any data that was created or modified after running **Generate Data Scramble Values**.

If you have a large volume of data for the fields you want to scramble, or plan to scramble many or all the available fields, Workday recommends that you create more than 1 scramble plan. Example: Instead of creating a single scramble plan with 150 fields, create 5 or 6 scramble plans with 25 to 30 fields per plan.

If you create multiple plans, run the **Generate Data Scramble Values** task followed by the **Start Data Scramble** task for each scramble plan consecutively. Processing each plan consecutively lessens the chance that you'll have inconsistent values based on the order that you generated scramble values from the different plans.

If you create more than 1 scramble plan that scrambles the same field or fields (Example: the First Name field), the last scramble plan you process overwrites scrambled field values from previous runs.

Related Information
Concepts
Refresh Tenant Request
Reference
Workday Community: Implementation Tenant Maintenance Windows

Data Security

Workday Key Management Service (KMS)

Concept: Key Management Service

The Workday Key Management Service (WD KMS) generates, stores, and manages cryptographic keys for securely encrypting and decrypting your tenant data.

Workday uses a root key to encrypt and decrypt other keys in the key hierarchy. Workday hosts your root key and generates other cryptographic keys using hardware security modules (HSMs). The HSMs:

- Adhere to the National Institute of Standards and Technology (NIST) 800-57 recommendations for key management.
- Are Federal Information Processing Standards (FIPS) 140-2 Level 3 compliant.

If you enable Workday Bring Your Own Key (BYOK), you:

- Create and host your own root key in your Amazon Web Services Key Management Service (AWS KMS).
- Enable Workday access on a per key basis.

Security Standards

Workday hosts hardware and stores sensitive cryptographic materials in secure environments. Additionally, Workday assigns specific roles and privileges to personnel, and their access is on a need-to-know basis. No individual has all critical knowledge or system access.

Workday separates the WD KMS from the environments and services that it serves. Workday also:

- Adheres to secure application development processes.
- Hosts the WD KMS infrastructure in a separate virtual local area network (VLAN) or virtual private cloud (VPC). Workday implements access controls that restrict traffic to the WD KMS.
- Segments keys by customer and tenant to ensure that you have your own hierarchy.

Key Lifecycle States

If you enable Workday BYOK, the key lifecycle states for the keys managed by you are the states inside your AWS account:

- Enabled, Disabled, PendingImport, PendingDeletion, Unavailable.

For the rest of the keys in the key hierarchy that Workday manages, cryptographic keys transition through the key lifecycle states in this table based on how long the keys exist and how protected your data is:

State	Description
Generated	Workday creates and securely stores the key without using it to encrypt and decrypt tenant data. A key in a Generated state can move to an Activated or Revoked state. Workday generates keys using NIST FIPS 140-2 Level 3 certified random bit generators.
Activated	Workday uses the key to encrypt and decrypt tenant data during its validity period. The validity period is 1 year from the key activation. A key in an Activated state can move to a Disabled or Revoked state.
Disabled	Workday uses the key to decrypt tenant data, but not to encrypt new data. A key in a Disabled state can move to a Revoked state.
Revoked	Workday doesn't use the key to encrypt or decrypt tenant data. Example: If Workday believes that your tenant data is in danger, Workday can temporarily move your cryptographic keys to a Revoked state. A key in a Revoked state can move to a Disabled state.

Note: If you perform an online restore or tenant refresh and select a source from a previous point in time, the data and keys revert back.

Key Hierarchy

Workday generates a hierarchy of cryptographic keys for managing access across all Workday services and SKUs. Each key is unique to your company. Workday uses most of the cryptographic keys to protect other keys in the key hierarchy.

Key	Description
Customer Key Encryption Key (CKEK)	Encrypts and decrypts the Customer Wrapper Key (CWK). The CKEK is a root key in the key hierarchy. Workday generates and stores the CKEK in a hardware security module. Workday generates CKEKs using NIST FIPS 140-2 Level 3 certified hardware security modules (HSMs).
BYOK Customer Key Encryption Key (BCKEK)	Encrypts and decrypts the Customer Wrapper Key (CWK) if you enable Workday BYOK in your tenant. If you enable Workday BYOK, you host your BCKEK in your AWS KMS, and enable Workday to access it. Workday doesn't use a CKEK if you use Workday BYOK. Workday also requires you to generate and host a Disaster Recovery BCKEK (DRBCKEK) in your AWS account. The DRBCKEK is a backup key for use if the BCKEK is inaccessible.
Customer Wrapper Key (CWK)	Encrypts and decrypts the Tenant Key Encryption Key (TKEK) and Customer Service Encryption Key (CSEK). If you enable Workday BYOK, Workday uses AWS KMS to generate the CWK, and then calls your BCKEK to encrypt the CWK. If you don't enable Workday BYOK, Workday generates the CWK from the HSM that Workday manages. We then store the CWK encrypted in the WD KMS.
Tenant Key Encryption Key (TKEK)	Encrypts and decrypts the Tenant Service Encryption Key (TSEK). Workday generates a TKEK for each tenant from the HSM and stores each TKEK in the tenant database. Example: If you have an implementation, sandbox, and production tenant, Workday generates and stores 3 separate TKEKs for the 3 tenants.
Tenant Service Encryption Key (TSEK)	Encrypts and decrypts your tenant data. Workday rotates the TSEK each year and stores each TSEK in the tenant database.
Customer Service Encryption Key (CSEK)	Encrypts and decrypts data shared across your tenants. Workday stores the CSEK in the WD KMS.

Workday Bring Your Own Key (BYOK)

Set Up Workday Bring Your Own Key (BYOK) For Amazon Web Services (AWS)

Prerequisites

- Acquire the BYOK SKU and agree to the applicable terms.
- Set up and configure the Amazon Web Services Key Management Service (AWS KMS).
- Open a support case in the Workday Customer Center for BYOK deployment to obtain the Workday user Amazon Resource Name (ARN) from Workday.

  Example: arn:aws:iam::123456789123: user/workday-kms-user.

  Note: Only your Named Support Contact can open the support case.

Context

Workday BYOK is an encryption key management capability that enables enterprises to take ownership and control of the keys they use for data encryption. The Bring Your Own Key Customer Key Encryption Key (BCKEK) is a root key that you generate and store in your AWS KMS. The BCKEK replaces the Customer Key Encryption Key (CKEK) in the key hierarchy and is used to encrypt and decrypt the Customer Wrapper Key (CWK).

Note: When you deploy Workday BYOK, it applies to all of your WD KMS-enabled tenants. Workday doesn't provide an option to revert to using Workday-issued encryption keys.

Workday requires that you create 2 keys in 2 different regions:

- A primary key for Workday to use as the BCKEK.
- A secondary key to use as the Disaster Recovery BCKEK (DRBCKEK) when the primary key is inaccessible.

Steps

1. In your AWS account, create a primary and secondary key.

   Both keys must be symmetric keys. Create the keys in the AWS regions specified in this table for your Workday tenant location. To secure the keys, follow the best practices recommended by AWS.

Workday Tenant Location	AWS Region for Primary Key (BCKEK)	AWS Region for Secondary Key (DRBCKEK)
WD1-PROD/WD2-IMPL, or WD12-PROD/WD12-IMPL	AWS us-east-2 (Ohio)	AWS us-west-2 (Oregon)
WD3-PROD/WD3-IMPL	AWS eu-west-1 (Ireland)	AWS eu-central-1 (Frankfurt)
WD5-PROD/WD5-IMPL	AWS us-west-2 (Oregon)	AWS us-east-2 (Ohio)
WD10-PROD/WD10-IMPL	AWS ca-central-1 (Canada Central)	AWS eu-west-1 (Ireland) In unique cases, you can place the DRBCKEK for WD10-PROD/WD10-IMPL in AWS ca-central-1 (Canada Central) instead.
WD102-PROD/WD102-IMPL	AWS ap-southeast-1 (Singapore)	AWS ap-southeast-1 (Singapore)
WD103-PROD/WD103-IMPL	AWS eu-central-1 (Frankfurt)	AWS eu-central-1 (Frankfurt)

Workday Tenant Location	AWS Region for Primary Key (BCKEK)	AWS Region for Secondary Key (DRBCKEK)
WD105-PROD/WD105-IMPL	AWS ap-southeast-2 (Sydney)	AWS ap-southeast-2 (Sydney)

Workday will specify additional AWS regions in the future to accommodate other Workday tenant locations.

2. Edit the key policy on both keys to give the user you obtained from Workday these permissions:
   - Encrypt
   - Decrypt
   - GenerateDataKeyWithoutPlaintext
   - DescribeKey

   Example:

```
{
"Sid": "Allow use of the key",
"Effect": "Allow",
"Principal": {
    "AWS": "arn:aws:iam::123456789123:user/workday-kms-user"
},
"Action": [
    "kms:Encrypt",
    "kms:Decrypt",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:DescribeKey"
],
"Resource": "*"
}
```

3. Using the support case you previously opened, provide the ARNs of the primary and secondary keys to Workday.

   Your Named Support Contact can submit the ARNs to Workday.
4. Confirm that the new keys are in use without any issues after the tenant reboots during the next Friday maintenance window.

Next Steps

If you wish to rotate your keys, repeat steps 1-3 above.

To remove access to your keys from Workday, either:

- Disable the keys inside AWS KMS.
- Keep the keys enabled and remove Workday permissions inside the key policy.

Once you remove access to a key that is in use and the rest of the key hierarchy is flushed out of caches, your tenants won't be accessible. The Tenant Key Encryption Key (TKEK) and Tenant Service Encryption Key (TSEK) get flushed out of the caches weekly when the tenant reboots during the Friday maintenance window. The CWK and Customer Service Encryption Key (CSEK) get flushed either during a WD KMS reboot, or after 7 days. In an emergency, Workday can flush out your cache without having to wait for 7 days or the Friday maintenance window.

After you restore Workday access, Workday can bring your tenants back online.

Any changes you make to the keys affect all your tenants. To revoke your keys and remove access from the data as soon as possible:

1. Revoke both the BCKEK and DRBCKEK in your AWS account.
2. Request Workday to shut down your tenants

Note: Never delete a BCKEK or DRBCKEK:

- If you delete both the BCKEK or DRBCKEK that's actively in use, Workday won't be able to recover the data in any of your tenants.
- If you delete both the old BCKEK and DRBCKEK, any backups that you created while that BCKEK and DRBCKEK were actively in use won't be recoverable.

For maximum safety, Workday recommends that you don't delete old BCKEKs and DRBCKEKs. Keep these old keys in the disabled state, which prevents their use but enables you to reactivate them in case of emergency.

Glossary

Full Glossary of Terms

A	B	C	D	E	F	G	H	I	J	K	L	M
N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Was this helpful?

A

Academic Date Range	The period of time associated with a student recruiting cycle.
Academic Level	The level of an educational objective that a student can pursue at an institution, such as: • Undergraduate, Graduate, or Professional at a university. • Associates or Baccalaureate at a community college.
Academic Unit	A Workday organization type that represents a school, college, university, or other unit of your institution. These units can recruit prospective students, admit students, offer programs of study or courses, or administer financial aid. Academic units are also used with academic appointments in Workday.
Academic Unit Hierarchy	A hierarchical grouping of academic units primarily used for roll-up reporting.
Accounting Cash	A group of cash ledger accounts that you can use to check cash balances against during settlement.
Accounting Cash Pool	One or more primary balancing worktag hierarchies that you can use to pool cash ledger balances for cash balance checks during settlement.
Active Candidate	A person with an application for a specific job requisition. Candidates must be linked to a job requisition for Workday to initiate a job application event.

All Ledgers Journal	An accounting journal that's not configured as a single ledger for the given company and is posted to both primary and alternate ledgers.
Applicant Pool	A subset of applications in an application grouping. Applicant pools enable you to control and adjust workload for application reviewers.
Application Grouping	A grouping of applications for the same admitting level of an academic unit and the same anticipated start date. Groupings can have 1 or more application pools, with an admissions counselor assigned to each pool.
Auto-fill	A time entry option that copies time blocks from a worker's schedule or from a previous week when entering time.
Award	A contract agreement with your sponsor in the form of funding to perform an activity for a public purpose. It defines how to capture direct and facilities and administration costs, recognize revenue, and bill your sponsor.
Award Costs Processing (ACP)	Processing facilities and administration costs and revenue recognition related to spend transactions on awards.
Award Credits	Percentage of award or award lines you allocate to specific worktags for reporting purposes.
Aggregation Security Group	A security group that grants access rights to members of an included set of security groups. Revokes access of members of any excluded security groups.
Approve	An action in a business process that designated participants select to progress the event to the next step.
Assignable Roles	Positions you can assign to organization roles.

Back to Top

B

Basis Limit	The maximum amount of direct costs you can use to calculate facilities and administration costs.
Base Pay Element	The compensation components that are included in the calculation of base pay for the purposes of determining the compa-ratio and target penetration. Example: Include both base pay and bonuses in the base pay calculation for compa-ratio.
Benefit Credit Bundle	A defined group of benefit credits that you can award together.

Benefit Defaulting Rule	A rule that identifies the benefit plans, coverage targets, and coverage amounts that employees receive by default when they do not complete an enrollment event.
Benefit Event Rules	These rules specify coverage increase limits, EOI requirements, waiting periods, and other rules and conditions of enrollment for benefits enrollment events.
Benefit Event Type	Identifies the events that trigger benefit enrollment, such as open enrollment, new hires, or the birth of a child. It also identifies the coverage types to make available to employees for when an event of this type occurs.
Benefit Group	A group of employees who qualify for benefits based on eligibility rules. Employees must be included in a benefit group to enroll in a benefit plan.
Business Object	Objects used to store data in Workday (such as organizations or workers). A business object has *fields* and *instances*, which are analogous to rows and columns in a spreadsheet. Workday links related business objects: a worker is associated with a position, the position to a job profile, and so on.
Business Process Definition	The tasks that compose a business process, the order in which they must be done, and who can do them.
Business Process Instance	A business process that the initiator has started. The *Hire Employee for Organization X* business process definition becomes an instance when the initiator uses it to hire an employee.
Business Process Security Policy	A business process security policy secures the steps and process-wide actions including view, rescind, cancel and correct. It specifies which security groups have access to each action.

Back to Top

C

Calculated Time	Result of applying time calculations to a worker's reported time. Automates application of company or regulatory rules.
Calendar-Based Time Entry	A time entry method that uses the time entry calendar as the focal point for entering, editing, and submitting time.
Cancel (business process)	Canceling a business process stops the workflow in progress and reverses changes made to data. You can't cancel a completed business process; you must rescind it. A securable action in a business process security policy.

Candidate	Candidates include both prospects and active candidates.
Candidate Pipeline	All active candidates.
Candidate Pool	Candidates grouped together based on specific criteria.
Cascading Leave	A sequence of related leave types that are linked together. When an employee meets the conditions defined for ending a leave, Workday generates a return from leave request and a separate request for the next leave.
Company	Companies are organizations within Workday that represent the internal business entities within your enterprise. In Workday Financial Management, companies are the primary organization for all business processes. A Company is considered the level at which one holds a balanced set of books and should reflect Legal Entities where possible.
Company Hierarchy	Defines a parent-child or reporting relationship between Companies in your organizations. The way that you structure your hierarchies influences many important Workday functions, especially role assignments, planning, and reporting.
Compensation Basis	A grouping of compensation components, such as salary, commission, and allowance plans, that define estimated earnings for an employee population.
Compensation Component	The umbrella term for compensation packages, grades, grade profiles, and plans that can be associated with compensation eligibility rules.
Compensation Defaulting Rule	A rule that establishes the criteria for how compensation components default to worker compensation during staffing transactions (such as hire or job change).
Compensation Element	Compensation elements link Compensation to Payroll. When a compensation element is attached to a plan that is assigned to an employee, Workday can determine which earnings to use to pay the employee.
Compensation Package	A grouping of compensation guidelines (grades, grade profiles, and their associated steps) and plans that you can assign to workers as a set. Packages provide a quick view of the eligible plans for a particular job or group of employees.
Compensation Rule	Guidelines for determining which workers are eligible for which components of compensation.
Compensation Step	A specific monetary amount within a grade or grade profile.
Compensation Target Rule	A rule used to segment your employee population for assignment of compensation plans.

Conditional Calculation	Time calculation that tags time blocks that meet certain conditions.
Conditions	Conditions are one or more logical matches that are resolved to True or False and used to decide if some action should be taken. You can add conditions to steps in a business process to determine if the step should run.
Connection Map	A tool on a customer profile that enables you to establish and manage the relationships between business entities and ship-to addresses.
Connector	A set of 1 or more integration templates that provide a framework for building integrations in a particular functional area. The integration can support a specific type of data, or can support a specific endpoint (example: Salesforce.com or Okta).
Consolidated Billing Schedule	A billing schedule type that allows you to combine all charges for multiple projects or services within a specific billing period into one invoice.
Contextual Custom Report	A custom report created from the related actions menu of a Workday object by selecting **Reporting > Create Custom Report from Here**. Simplifies choices of data and fields to those related to the context of the object.
Contract Rate Sheet	A document that outlines the contract billing hourly rates for roles such as the engineer, manager, or consultant, with the option to add billing rules for specific contract considerations.
Conversation Tag	A descriptor, such as Dietary Restrictions or Special Needs that you can assign to an engagement conversation to identify its topic. You can search for conversations by conversation tag.
Conversation Topic	A conversation tag or recruiting event name that you can associate with an engagement conversation to make conversations easier to find.
Correct (business process)	Correcting a business process changes a specification or data in the workflow while in progress. A securable action in a business process security policy.
Cost Reimbursable Spend	A billing item that Workday creates to help you bill your sponsor for award-related spending. The cost reimbursable spend amount includes both the original spend amount and any overhead costs Workday calculates based on your award costs configurations.
Coverage Target	Defines whether a specific health care plan or insurance plan applies only to the employee or also to the dependents, spouse, family, and so on.
Cross Plan Dependency	Limits the coverage options available to workers during an enrollment event based on their choice of other benefit plans and coverage amounts.

	Example: You can limit coverage in a specific plan to a percentage of the total coverage in 1 or more other benefit plans.
Custom Report	Reports not delivered by Workday and built using the Workday Report Writer. Can be created new or by copying another standard or custom report.
Customer Payment Matching	A feature that uses historical payment applications to suggest customer invoices and adjustments that match customer payments with insufficient remittance advice.
Customer Refund Payments in Settlement Runs	A refund payment generated by the settlement run with a payment date that reflects the date you settle the refund.

Back to Top

D

Dashboard (landing pages)	A specialized landing page containing a set of pre-configured worklets for a functional area that you can copy or modify. You can add additional custom worklets to dashboards using the report writer.
Data Source	A data source defines a set of business object instances for reporting purposes. Allows reporting access to all business objects related to those in the data source.
Day Breaker	The time of day on which a worker's work day and work week begins. Defines the 24-hour period over which daily time calculations execute and the 168-hour period over which weekly time calculations execute. Unless otherwise specified, the default day breaker is 12am.
Deny (business process)	When you deny a business process, the business process is terminated and all Workday data is restored to its state before the business process started. To restart the business process, you need to submit the process again, and redo all previously completed steps.
Depreciation Profile	A configuration that determines how Workday depreciates assets by defining a depreciation method, convention, and useful life.
Designation	An attribute, such as Community Learning Partner, Honors, or STEM, that you can associate with educational institutions and external associations to make them easy to find and report on.
Discrete Composite Asset	A combination of related but distinct assets for which you can individually track cost, depreciation, and lifecycle events.
Disposition	Status of candidates that have been rejected for hire or declined a job during the job application event.

Domain	A collection of related securable items such as actions, reports, report data, report data sources, or custom report fields. Each domain is secured by a domain security policy.
Domain Security Policy	A collection of related securable elements of different types and user-specified security groups that have access to elements of each type.
Dynamic Period	A date that identifies the anticipated start date for a student of online education or other asynchronous learning.

Back to Top

E

Educational Taxonomy	A taxonomy scheme and set of codes you can assign to programs of study and their concentrations to meet state, local, or other classification requirements.
Eligible Investigator	A type of role that you can use to assign individuals to awards, grants, and grant hierarchies, so that the role assignments remain intact even when the person's position or organization changes.
Engagement Action Item	Defines a requirement that must be met for an application for admission to be considered complete. Example: Submit transcripts.
Engagement Item	An engagement email or printed engagement item. You can include engagement items in engagement plans and use them to support student recruiting events.
Enrollment Event Rule	A rule that defines coverage start and end dates, waiting periods, coverage increase limits, Evidence of Insurability requirements, and other coverage rules and conditions. Rules ensure that the benefits process presents only the options that each employee is eligible for based on the event type.
Enterprise Interface Builder (EIB)	An integration tool that enables you to create simple, secure, and customizable integrations with Workday. Alternately, an EIB is a simple integration created by the integration tool. An EIB consists of an integration system, an integration data source, an integration transformation, and an integration transport protocol.
Estimate at Completion (EAC)	Includes all the hours logged and approved for the project, as well as the future hours the worker expects to complete.
Estimate to Completion (ETC)	Includes the future hours the worker expects to complete.
Event	A business process transaction that occurs within your organization, such as hiring or terminating an employee.

External Association	A nonprofit, community-based, or other noneducational organization that you can associate with student prospects or identify as a location for recruiting events.
External Engagement Item	Used to send and track third-party engagement items for recruiting events, communication plans, or ad hoc communications.

Back to Top

F

Fast Path	A streamlined approach to moving applications for admission from submission to matriculation as quickly as possible.
Field Overrides	A tool that lets you customize integration systems that are based on a connector template. Field overrides are managed through an integration service. They use calculated fields or report fields to supply values to an integration system. Example: member IDs in benefit provider integrations.
Financial Aid Period Record	A record containing data such as academic unit, academic level, and program of study for a student that Workday uses to process financial aid for an academic period.
Functional Area	A collection of domain or business process security policies that are related to the same set of product features, for example, Benefits or Compensation.

Back to Top

G

Grade Profile	A breakdown of a compensation grade by functional task, geographical region, or other categorization your business requires. A profile enables you to assign more granular compensation ranges to workers.
Grant	A worktag that you can use to capture award-related expenses.

Back to Top

H

Headcount Plan	Provides visibility into the number of workers necessary to achieve your business goals within a specified period of time.

Back to Top

I

Individual Target	An individual bonus or merit target for a worker during a compensation review process that

	overrides the target defined on the compensation plan.
Integration Attribute	An integration component that specifies the tenanted value of a data element in Workday. Example: Plan Sponsor Name is a type of attribute in benefit provider integrations.
Integration Data Source	Indicates the type of data that Workday receives from or exports to an external system and its location.
Integration Event	The record of an integration process. Every integration—current or past, involving the import or export of data, successful or not—gets recorded as an integration event. The integration event contains all the information about the integration process, including its status.
Integration Map	An integration component that specifies how values in Workday map to values in an external system. Example: Pay Rate Frequency is a type of map in third-party payroll integrations.
Integration Service	A group of related integration attributes, maps, and XSLT that provides a framework to transform Workday data into the format required by an external system.
Integration System	A tenanted definition of an integration between Workday and an external system based on a template that provides the methodology for communicating data.
Integration Template	A collection of integration services that enables communication between Workday and an external system. Workday provides integration templates in categories such as Benefits, Financials, HCM, Payroll, Payroll Interface, Procurement, Recruiting, Security, and Settlement. Many of the delivered templates contain default values for attributes, as well as prompt values for attributes and maps, to define the integration further.
Integration Transformation	Converts data into a format that Workday or a receiving external system can understand. Workday provides some delivered transformations, and you can also create custom transformations.
Integration Transport Protocol	Controls how Workday exports data to an external endpoint or service or imports the data from an external endpoint or service. Workday supports several types of transport protocols, including email, FTP and SFTP, HTTP/SSL, Workday attachments, and Workday Web Services.
Intersection Security Group	A security group whose members are other security groups. Members associated with all included security groups are granted access through an intersection security group.

Initiation Step	The first step of a business process.

Back to Top

J

Job-Based Security Group	A security group that includes one or more job-related attributes or objects including job profile, job family, job category, management level, or exempt/non-exempt status.
Job Management Staffing Model	A structure that defines 1 set of hiring restrictions for all jobs in a supervisory organization, with no specific limits on the number of jobs that can be filled.
Job Profile	The generic features and characteristics of a job or position, such as management level, pay rate type, compensation, skills, and other qualifications.

Back to Top

K

Knowledge Article	An article that is accessible to workers in your organization based on the assigned article audience. You can use these articles to document, share, and manage HR information specific to your organization.
Knowledge Article Audience	A group of employees that can view designated Knowledge articles. Their access to articles is determined by condition rules assigned to the audience.

Back to Top

L

Landing Page	Landing pages display a collection of worklets. Landing pages may have different display formats (grid or bubble) and support different functions. The Home landing page is intended for common worklets, such as self-service worklets.
Leave Family	A set of similar leave of absence types. Example: A company-specific family includes disability leave and bereavement leave, while a separate regulatory family includes jury duty and family medical leave.
Leave of Absence Rule	A rule that defines worker eligibility for leaves of absence.
Line Tax Rate Application (LTRA)	A collection of tax amounts that apply to a given transaction line or supplier invoice line split on a taxable document.
Linked Customer Contracts	Child customer contracts that you associate with a parent customer contract for revenue allocation purposes.

Linked Leave	A leave type that shares an entitlement with other leave types or time offs. Eligibility rules, validation rules, and supporting data reference the combined balance of the associated leave types and time offs. Also known as coordinated leaves and time off.
Location Membership Security Group	A security group whose members are any workers assigned to that location.

Back to Top

M

Match and Merge	A process that helps eliminate duplicate student prospect information in Workday.
Micro-edit	The ability to edit existing time blocks or add time blocks directly to a day by clicking the time entry calendar.
Multiplier-Based Coverage	Insurance coverage based on multiples of salary, such as 1x, 2x, or 3x salary.

Back to Top

N

Nonbillable	A nonbillable project is an internal project that you don't invoice customers for.

Back to Top

O

Object Class	The spend categories that award sponsors agree to reimburse award recipients for maintaining their projects.
On-Account Document	A document that’s generated when you place a payment amount on an existing customer account. You can apply on-account documents to future payments.
Organization Security Group	A security group whose members are any workers assigned to that organization.

Back to Top

P

Parent Customer Contract	A customer contract that you associate with a child customer contract so you can add contract lines across contracts to the same schedule. When you view the parent customer contract, Workday displays the child customer contracts as linked contracts.
Passive Event	Events that result from the passage of time rather than from a specific change to employee data.

Payment Group	The payments that result from a settlement run.
Payment Tax Rate Application (PTRA)	A collection of tax amounts that apply to a given payment on a taxable document.
Position Management Staffing Model	A structure that defines different staffing rules and restrictions for each position in an organization.
Position Restrictions	The attributes and conditions that apply to an unfilled position in a supervisory organization that uses the position management staffing model. Example: Job profile, location, qualifications, and worker type.
Pre-Hire	In Staffing, an individual you're tracking before employment. In Recruiting, a candidate who is in the *Offer*, *Employment Agreement*, *Background Check*, or *Ready for Hire* stage.
Procurement Contract	Contracts enable your organization to define preferred suppliers, analyze spend for better control, and standardization. They also allow your organization to implement contractual spend to better negotiate and enforce discounts and other supplier terms.
Procurement Contract Type	A procurement contract in Workday is always associated with a Contract Type that dictates how the contract can be used across the procure-to-pay chain. Example: when a Contract Type has the **Scheduled Purchase Orders** option set, Workday can use the contract to automatically create purchase orders based on a predefined schedule.
Project Advanced Labor Costing	Prorating project labor costs using standard or fully burdened costing.
Project Asset	A container that captures separate, ongoing costs of a capital project in progress. You can associate multiple projects assets with a project to track costs over the life of a project.
Project Billing Rate Sheet	A document that outlines the hourly or daily rates charged per project role, with the option to be more specific based on defined categories such as Region, Skill Level, and Project Size.
Project Plan Phase	A phase in the project plan that represents a stage in the project work. Example: Plan and Strategize. A project plan organizes projects into sequenced phases and tasks. A project phase is generally project agnostic, but when you add that phase into a project plan, it becomes a project plan phase.
Project Plan Task	The work details in a project plan phase. Example: Define Project Objectives.
Project Transaction Source	The source of project billing transactions. Example: Supplier Invoice, Expense, or Time.

Prospect	Someone you are interested in tracking who isn't associated with a specific job. You can use tags, prospect types, and prospect statuses to help track these individuals.

Back to Top

Q

Quick Add	A time entry option that enables you to create a time block and copy it to multiple days in a week.

Back to Top

R

Recipient Threshold	The maximum number of prospects to whom you can send an engagement item at the same time without requiring approval.
Recruiting Cycle	A recruiting period for 1 or more academic levels of an academic unit. You associate recruiting cycles with campaigns to measure the effectiveness of each campaign per recruiting cycle.
Reference ID	A unique identifier used to look up data for integration purposes.
Reference Pay Range	A range of pay established for a compensation grade or grade profile.
Related Customer Contract	A customer contract that you associate with another customer contract for reporting purposes. When you create a customer contract, you can associate 1 related customer contract with it. The related customer contract must share the same company and sold-to customer.
Reported Time	A worker's time that has been entered, but has not had any time calculations applied.
Revenue Category	An attribute in customer contracts and billing used to search for and report on goods and services you sell. Also a dimension in account posting rule types for customer contracts, billing, and accounts receivable that drives accounting behavior.
Risk Insight	Provides the reason why Workday identifies an expense report with a High or Medium risk level. Reasons may include 1 or more of these: Amount Anomaly, Duplicate Expense, and Incorrect Expense Item.
Risk Level	The value (Low, Medium, and High) that Workday provides from risk evaluation. Workday provides default risk levels, which can also be configured based on Risk Score.
Risk Score	The numerical value (0 to 100) that Workday provides from risk evaluation. The score helps identify anomalous expense reports.

Back to Top

S

Single Ledger Journal	An accounting journal that's a single primary or alternate ledger currency for the given company.
Source	The duplicate record that you want to merge in the Duplicate Management Framework.
Spend Category	A logical grouping to search and report on acquired items and services. Also a dimension in account posting rules for procurement and spend that drives accounting behavior.
Staffing Model	A structure that defines how jobs and positions are created and filled in a supervisory organization. Workday supports 2 kinds of staffing models: • Job management. • Position Management.
Staffing Organization	An organization category that includes supervisory organizations, matrix organizations, or retiree organizations.
Stage	A value, such as Lead, Inquirer, or Applicant, that identifies where a student prospect is in the recruitment or admissions process.
Student Financials Period Record	A record containing data such as academic unit, academic level, and program of study for a student that Workday uses to process student financials transactions for an academic period.
Student Prospect Profile	A worklet that displays information for a prospective student, including contact information and recruitment details.
Student Prospect Type	A value, such as First Year or Adult Returning, that you can assign to prospective students and use to match student prospects to admissions counselors automatically.
Student Recruiting Region	Workday term for recruiting territory. A recruiting region can represent a geographical area, 1 or more schools, or schools in selected school districts.
Student Tags	An attribute, such as Veteran, Athlete, or Scholarship Recipient, that you can assign to student prospects. You can use tags to match student prospects to recruiters automatically, find prospects, and use as criteria for associating engagement plans with prospects.
Supplier Contract	Contracts enable your organization to define preferred suppliers, analyze spend for better control, and standardization. They also allow your organization to implement contractual spend to better negotiate and enforce discounts and other supplier terms.

Supplier Contract Type	A supplier contract in Workday is always associated with a Contract Type that dictates how the contract can be used across the procure-to-pay chain. Example: when a Contract Type has the **Scheduled Purchase Orders** option set, Workday can use the contract to automatically create purchase orders based on a predefined schedule.
System User	An account associated with and required to launch a Connector or Studio integration. Workday delivered integrations and custom integrations require a system user account for authentication and web service calls. A system user account is not associated with a person in Workday.
Staffing Organization	An organization category that includes supervisory organizations, matrix organizations, or retiree organizations.

Back to Top

T

Target	The record into which you want to merge the source in the Duplicate Management Framework.
Tax Code	A combination of tax rates that you select on transaction lines.
Tax Rate Application (TRA)	A collection of tax amounts across all lines on a taxable document with the same tax applicability, tax code, tax option, tax point date, tax rate, and tax recoverability.
Tax Recovery Pro Rata Factor Percentage	A company-specific percentage that modifies the tax recoverabilities that you configure for the tenant.
Termination Adjustment	A time off adjustment that automatically sets the remaining balance of a worker's time off plan to zero upon the worker's termination.
Time Block	A time block carries information about a portion of time, such as the number of hours worked or in/out times. Time blocks can be reported or calculated, but only calculated time blocks are pulled into Workday Payroll.
Time Calculation	A set of rules to apply time calculation tags to calculated time blocks for Payroll or other purposes. Example: You could create a time calculation to convert regular hours into overtime hours automatically if a worker works more than 40 hours in a week.
Time Calculation Tag	Workday applies calculation tags to time blocks during time calculations. The tags map to payroll earnings to drive how time blocks are paid and can be included in time off and accrual calculations. You can also use them to display time and time off totals on the time entry calendar.

Time Clock Event	A time clock event describes a worker's actions, such as a check-in or check-out, on the web time clock or an external time clock. Workday matches time clock events to form time blocks, which workers can edit and submit.
Time Code Group	The primary use of a time code group is to determine which time entry codes a worker is eligible for. Time code groups are assigned to a worker or to a position through eligibility rules.
Time Entry Calendar	A set of self-service pages that workers use to enter, edit, and submit time, when using calendar-based time entry. When using high volume time entry, workers can view and submit time from the time entry calendar.
Time Entry Code	A time entry code describes the type of time a worker enters, such as worked time or meal allowance. To use time entry codes, you must attach them to time code groups, except for the default time entry code assigned to a time entry template.
Time Entry Template	A template defines how a worker's time entry calendar is configured. Workers are matched to time entry templates through eligibility rules.
Time Entry Validation	Errors or warnings that prevent users from entering invalid time. Critical validations prevent a user from submitting time. Warnings display when entering time but don't prevent the worker from submitting time.
Time Off	The rules that apply to a specific type of time off, including eligibility rules, whether adjustments are allowed, and limits that differ from the time off plan.
Time Off Plan	The rules for entering and tracking 1 or more related time offs. Identifies the unit of time, eligibility requirements, whether to track balances, and if time offs are position-based or worker-based.
Time Period Schedule	A time period schedule defines which dates are available for entry at a given time and defines which dates are paid in which pay periods. They can line up with pay periods, or, in more complex scenarios, they can be paid on a lag.
Time Proration Rule	A rule that prorates employees' target compensation in a bonus or merit increase compensation event according to time-based criteria, such as leave of absence or time since hire.
Time Shift	A grouping of consecutive time blocks that you can use in standard overtime calculations, time block conditional calculations, and validations.

Back to Top

U

Unbillable	An unbillable transaction is a billing transaction that has an issue preventing it from being billed. You can't take action on the transaction until you resolve the issue.
Unnamed Resources	Placeholders for project resources that you can use to assign tasks and perform resource forecasting without specific resource assignments.

Back to Top

V

Value-Based Project	A customer contract line type that you use when your project billing installment values are not known at the time of contract creation.

Back to Top

W

Wave Picking	Enables you to group picking lists together in groups to better organize and prioritize your inventory picking process
Week Breaker	The day of the week on which a worker's work week begins. Defines the 7-day period over which weekly time calculations execute. Unless otherwise specified, the default week breaker is Sunday at 12am.
Work Schedule Calendar	A calendar that defines the days and hours that a worker is scheduled to work. In Time Tracking, work schedule calendars affect time entry options, calendar displays, and time calculations.
Workday Studio	An Eclipse-based development environment that enables you to build more complex integrations with Workday.
Workday Web Services	Workday’s public API. Based on open standards, Workday Web Services (WWS) provide the core method for integration with Workday.
Worker	An employee or a contingent worker.
Worklets	Mini applications represented by clickable icons in Workday, providing quick and easy access to tasks and data that you access regularly. Example: the Inventory or Time Off worklets, or a worklet based on a report.

Back to Top

X

No Entries

Back to Top

Y

No Entries

Back to Top

Z

Zone Picking	A method of picking for orders from different zones at an inventory site. In Workday, you can split a stock request into multiple zone picking lists for more efficient picking and shipping. You can then ship the zone picking lists separately or merge them before shipment.

Back to Top