IBM Security Verify Governance Identity Manager

v10.0

Workday HR Feed Adapter Installation

And

Configuration Guide

Table of Contents

Chapter 1. Overview

An Adapter is an interface between a managed resource and the IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server. The Workday HR Feed Adapter enables communication between the IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server and the Workday HR target.

Features of the adapter

The adapter is designed to create WorkdayHR Persons in IBM Security Verify Governance Identity Manager using worker, organization and other supporting data that it reconciles from Workday.

This adapter is not designed to create, update, delete or otherwise maintain accounts, Workday workers, Workday organizations or other Workday supporting data types.

Architecture

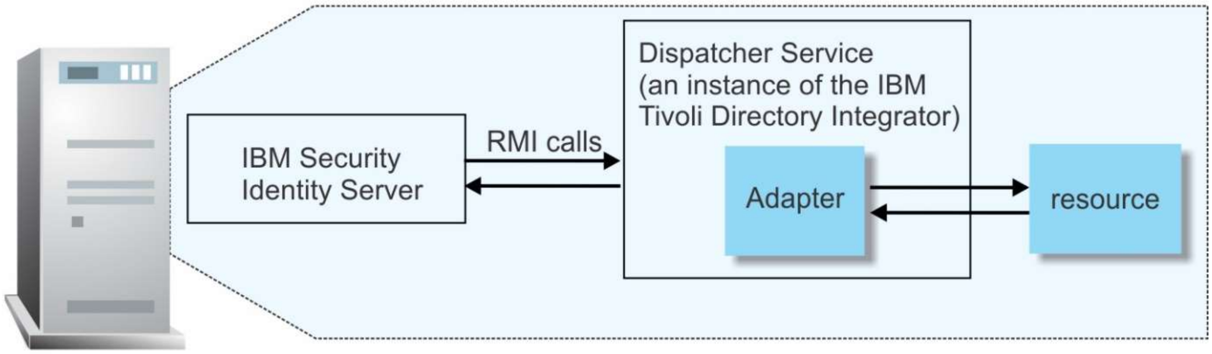
Several components are involved while running and using the adapter. Install all these components so that the adapter can function correctly.

The adapter requires the following components:

- Dispatcher
- IBM Security Directory Integrator connector
- Workday HR Feed Adapter

Figure 1 describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

Figure 1. The architecture of the Workday HR Feed Adapter



Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

- An IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server
- An IBM Security Directory Integrator server
- The managed resource
- The Workday HR Feed Adapter

The adapter must be installed directly on the server that runs the Security Directory Integrator server.

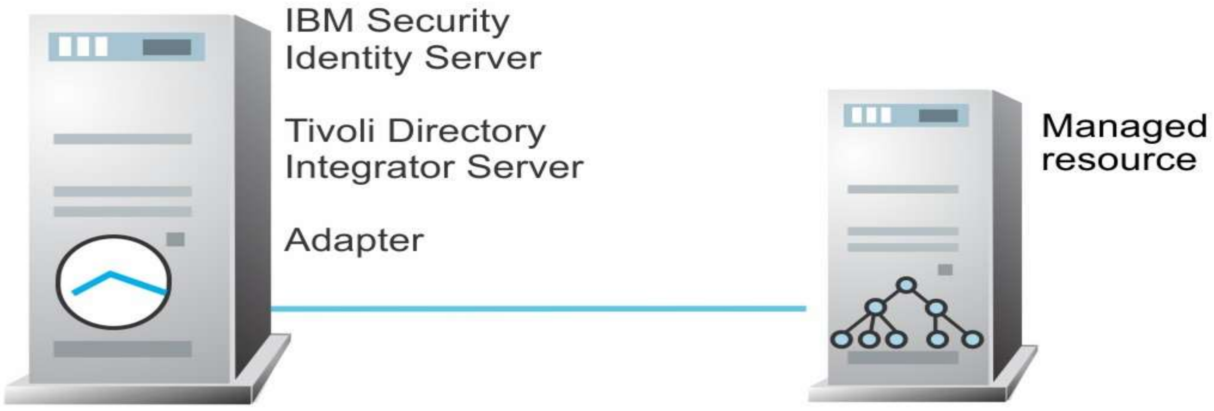
Single server configuration

In a single server configuration, the following components are installed on one server to establish communication with the Workday HR managed resource:

- An IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server
- Security Directory Integrator server
- Workday HR Feed adapter

The Workday HR resource resides externally as shown in Figure 1.

Figure 1. Example of a single server configuration



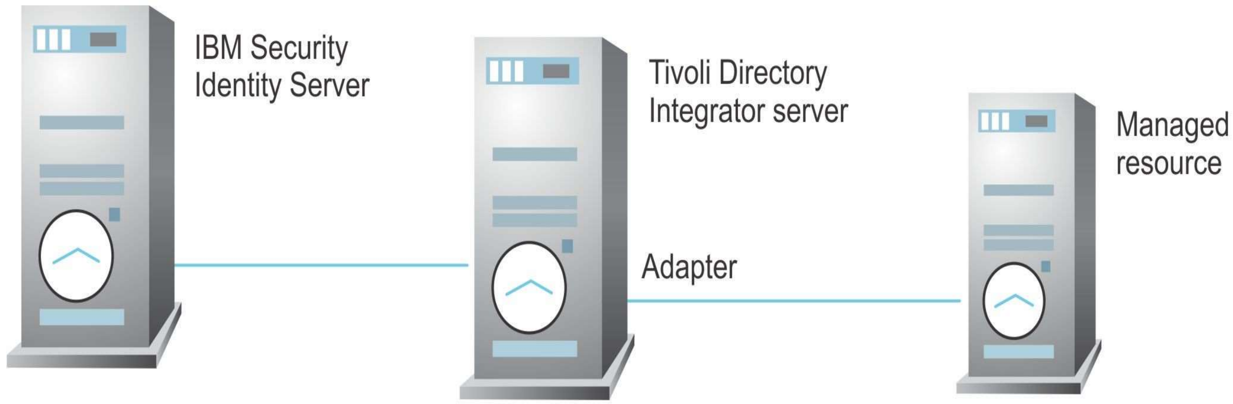
Multiple server configuration

In a multiple server configuration, the following components are installed on different servers.

- An IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server
- Security Directory Integrator server
- Workday HR Feed Adapter
- Managed resource

The Security Directory Integrator server and the Workday HR Feed Adapter are installed on the same server as shown in Figure 2.

Figure 2. Example of a multiple server configuration


IBM Security Identity Server
Tivoli Directory Integrator server
Adapter
Managed resource

Chapter 2. Planning

Installing and configuring the adapter involves several steps that you must complete in a specific sequence. Follow the roadmap for the main tasks.

Roadmap for IBM Security Directory Integrator based adapters

Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Pre-installation

Complete these tasks.

1. Verify that your environment meets the software and hardware requirements for the adapter. See Prerequisites.
2. Obtain the installation software. See Software downloads.
3. Obtain the necessary information for the installation and configuration. See Installation worksheet.

Installation

Complete these tasks.

1. Installing the dispatcher
2. Installing the adapter binaries or connector
3. Verifying the adapter installation
4. Restarting the adapter service
5. Creating a Service Account/API Client in Workday
6. Configuring the SSL connection between the Dispatcher and the Workday HR tenant
7. Importing the adapter profile
8. Creating an adapter service/target
9. Service/Target Form details
10. Verifying that the adapter is working correctly
11. Installing ILMT-Tags

Upgrade

To upgrade the adapter, do a full installation of the adapter. Follow the Installation roadmap.

Configuration

Complete these tasks.

1. Configure secure communication between the IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server and the adapter.

   a. Configure 1-way authentication.
   b. Configure 2-way authentication.

2. Configure secure communication between the adapter and the managed target.
   a. Configure 1-way authentication.
   b. Configure 2-way authentication.
3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

- Techniques for troubleshooting problems
- Error messages and problem solving
- Enabling DEBUG Logs on SDI Server

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Delete the adapter service/target.
4. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes

Pre-Requisites

Verify that your environment meets the software and hardware requirements for the adapter. Consult the release notes for currently supported versions.

Table 1 identifies the prerequisites for the adapter installation.

Table 1. Prerequisites to install the adapter

Prerequisite	**Description**

Directory Integrator	• IBM Security Directory Integrator
IBM Security Verify Governance Servers	The following servers are supported: • IBM Security Verify Governance Identity Manager • IBM Security Verify Governance
IBM Security Directory Integrator adapters solution directory	An IBM Security Directory Integrator working directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*.
System administrator authority	You must have system administrator authority to complete the adapter installation procedure.

Software downloads

Log in to your account on the IBM Passport Advantage website and download the software.

Go to IBM Passport Advantage. See the corresponding IBM Security Verify Governance Identity Manager or Security Verify Governance server Download Document for instructions.

Note: You can also obtain adapter information from IBM Support.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 1. Required information to install the adapter

Required information	**Description**	**Value**

IBM Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory, which contains the files for the adapters.	**Windows:** drive\Program Files\IBM\TDI\V7.2 **UNIX:** /opt/IBM/TDI/V7.2
Adapter Solution Directory	When you install the dispatcher, the installer prompts you to specify a filepath for the solution directory. For more information, see the *Dispatcher Installation and Configuration Guide*.	**Windows:** drive\Program Files\IBM\TDI\V7.2\timsol **UNIX:** /opt/IBM/TDI/V7.2/timsol
Create a Service User / API Client on the Workday HR managed resource	A Service User / API Client must be created with the required access for performing reconciliation of the Worker accounts, Organizations and Support data from Workday HR managed resource.	

Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

Installing the dispatcher

If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

If you already installed the RMI Dispatcher for another adapter, you do not need to reinstall it.

If you have not yet installed the RMI Dispatcher in the Security Directory Integrator environment, download the Dispatcher installer from the IBM Passport Advantage website. For more information about the installation, see the Dispatcher Installation and Configuration Guide.

Installing the adapter binaries or connector

The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Before you begin

- The Dispatcher must be installed.

Procedure

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the WorkdayConnector.jar file from the adapter package to the ISDI_HOME\jars\connectors directory.
4. Copy the com.ibm.jaxws.thinclient*.jar file from the adapter package to the ISDI_HOME\jars\3rdparty\others directory.
5. Restart the adapter service.

Verifying the adapter installation

After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter connector and JAX-WS ThinClient JAR files exists in the specified directories. If the JAR files doesn't exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified locations.

Windows operating system

drive:\Program Files\IBM\TDI\V7.2\jars\connectors\

drive:\Program Files\IBM\TDI\V7.2\jars\3rdparty\others\

UNIX operating system

/opt/IBM/TDI/V7.2/jars/connectors/

/opt/IBM/TDI/V7.2/jars/3rdparty/others/

If this installation is to upgrade a connector, then send a request from IBM Security Verify Governance Identity Manager or IBM Security Verify Governance. Verify that the version number in the ibmdi.log matches the version of the connector that you installed. The ibmdi.log file is at ISDI_Home\adapter solution directory\logs.

Restarting the adapter service

Various installation and configuration task might require the adapter to be restarted to apply the changes.

For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Security Directory Integrator instance.

See the topic about starting, stopping, and restarting the Dispatcher service in the Dispatcher Installation and Configuration Guide.

Creating a Service Account/API Client in Workday

Before you create a Workday HR Feed connector, you must obtain Service Account / API Client details for the Workday HR Feed Adapter.

Before you begin

Ensure your Workday Account has permissions to create a service account and API client in Workday target.

About this task

To create a service for the Workday HR Feed Adapter, you specify the connection and authentication details. To populate those fields, you must create a service account and API Client in Workday based on the required type of authentication. All these tasks needs to be performed in Workday target.

Creating Integration System User (ISU)

About this task

This task needs to be completed for all authentication types.

Note: For OAuth using Refresh Token, ISU is not required on the Adapter Service/Target Form, however, it is still needed to complete the API Client Setup.

Procedure

1. In Workday, execute **Create Integration System User** task.
2. Enter the required details for Account Information in the task (User Name, Password, etc) for adapter service account. (For example: IBM_HR_Adapter_User)

   Note: Please make a note of the Password for Basic Authentication. For other authentication types, password is not required on Adapter Service/Target Form. Also, select **Do Not Allow UI Sessions** to not allow the ISU for logging into Workday through UI.

Creating Integration System Security Group (ISSG)

About this task

This task needs to be completed for all authentication types.

Note: Details entered to complete this task is not required on the Adapter Service Form, however it is still required to complete this task for the adapter to function properly.

Procedure

1. In Workday, execute **Create Security Group** task.
2. Select **Integration System Security Group (Unconstrained)** or **Integration System Security Group (Constrained)** type and assign a name to the Security Group. (For example: IBM_HR_Adapter_Group)
   The main difference between Unconstrained and Constrained types is that constrained security group will only return results for objects that have a connection with constraint.
3. Add newly created ISU (For example: IBM_HR_Adapter_User) to this security group.

Assigning Domain Security Policy Permissions to Integration System Security Group

About this task

This task needs to be completed for all authentication types.

Procedure

1. In Workday, run **View Security Group** report.
2. Select the **Integration System Security Group** created in the previous task. (For example: IBM_HR_Adapter_Group)
3. From the **Action** items, select **Maintain Permissions for Security Group** under **Security Group**.
4. Select below security policies under **Domain Security Policies permitting Get access** and click on **OK**:
    a. Worker Data: Public Worker Reports
    b. Manage: Organization Integration
    c. Job Information
    d. Manage: Location
    e. Set Up: Contact Info, IDs, and Personal Data
    f. Person Data: Personal Information
    g. Person Data: Date of Birth
    h. Person Data: Birth Place
    i. Person Data: Gender Identity
5. Click on **Done**.
6. Execute **Activate Pending Security Policy Changes** task.
7. Describe changes in the **Comment** and click on **OK**.
8. Select **Confirm** checkbox and click on **OK** to activate these changes.

Generating a Public/Private Key Pair and Keystore

About this task

This task needs to be completed only for OAuth using JWT, X509 and SAML authentication types. This task provides procedure with keytool as a sample, however any other tool can also be used.

This task also provides the steps to create x509 public key in Workday.

Procedure

1. Generate a key pair and store it in a key store called **WorkdayKeystore.jks** with any password (For example: Workday123!) using below command:

    ```
    keytool -genkey -keyalg RSA -alias Workday -keystore WorkdayKeystore.jks -storepass Workday123!
    -validity 360 -keysize 2048
    ```

2. Extract the public key and save it to a file called **publickey.cert** using below command:

    ```
    keytool -export -alias Workday -keystore WorkdayKeystore.jks -rfc -file publickey.cert
    ```

3. In Workday, execute Create x509 Public Key task.

4. Provide a **Name** for the certificate. (For example: IBM_HR_Adapter_Pub_Key)
5. Copy the content of **publickey.cert** file exported in step 3 to **Certificate** field and click **OK**.
6. Click **Done**.

Configuring Web Service Security for the Integration Service User (ISU)

About this task

This task needs to be completed only for X509 or SAML authentication types.

Procedure

1. In Workday, execute **Configure Web Service Security** task.
2. Select ISU created in the earlier task. (For example: IBM_HR_Adpater_User)
3. For **SAML** authentication type complete below details under **SAML Token Configuration** and click **OK**:
    a. Select the checkbox for **Enable SAML Authentication**.
    b. Provide a name for **SAML Identity Provider**. (For example: IBM_HR_Adapter)

       This value needs to be provided in **Workday Issuer ID** on the Adapter Service Form.
    c. Select **Identity Provider's Public Key** that was created in previous task. (For example: IBM_HR_Adapter_Pub_Key)
4. For **X509** authentication type complete below details under **X509 Token Configuration** and click OK:
    a. Select the checkbox for **Enable X509 Token Authentication**.
    b. Select **X509 Public Key** that was created in previous task. (For example: IBM_HR_Adapter_Pub_Key)
5. Click **Done**.

Creating an API Client for OAuth using JWT

About this task

This task needs to be completed only for OAuth using JWT authentication type.

Procedure

1. In Workday, execute **Register API Client** task.
2. Provide a **Client Name**. (For example: IBM_HR_Adpater_Client)
3. Select **Client Grant Type** as **Jwt Bearer Grant**.
4. Select **x509 Certificate** that was created in previous task. (For example: IBM_HR_Adapter_Pub_Key)
5. Select **Access Token Type** as **Bearer**.
6. Select **Scope (Functional Areas)** listed below and click **OK**:
    a. Staffing
    b. Organizations and Roles
    c. Jobs & Positions

    d. Contact Information

7. Note the value for **Client ID** as this will be required on the adapter service form and Click **Done**.

Creating an API Client for OAuth using Refresh Token

About this task

This task needs to be completed only for OAuth using Refresh Token authentication type.

Procedure

1. In Workday, execute **Register API Client for Integrations** task.
2. Provide a **Client Name**. (For example: IBM_HR_Adpater_Client)
3. Select the checkbox for **Non-Expiring Refresh Tokens**.
4. Select **Scope (Functional Areas)** listed below and click **OK**:
    a. Staffing
    b. Organizations and Roles
    c. Jobs & Positions
    d. Contact Information
5. Note the value for **Client ID** and **Client Secret** as this will be required on the adapter service form and click **Done**.
6. Run **View API Clients** report.
7. From **API Clients for Integrations** tab, select the API client created above. (For example: IBM_HR_Adapter_Client)
8. From **Actions**, select **Manage Refresh Tokens for Integration** under **API Client**.
9. Select the Workday Account generated in the earlier tasks. (For example: IBM_HR_Adapter_User)
10. Select the checkbox for **Generate New Refresh Token** and click **OK.**
11. Note the value for generated Refresh Token as this will be required on the adapter service form and click **Done.**

Configuring the SSL connection between the Dispatcher and the Workday HR tenant

To enable communication between the adapter and the Workday HR tenant, you must configure keystores for the Dispatcher.

About this task

For more information about SSL configuration, see the Dispatcher Installation and Configuration Guide.

Procedure

1. Open a web browser and go to https://www.digicert.com/kb/digicert-root-certificates.htm
2. Download the DigiCert Global Root G2 certificates in DER/CRT format.
3. Export the certificate into a file that is encoded in the Base64 format.
4. If the Dispatcher already has a configured keystore, use the iKeyman Utility to import the DigiCert

Global Root G2 certificate.

   a. Navigate to the ISDI_HOME/jvm/jre/bin directory.
   b. Start the ikeyman.exe file.
   c. From the **Key Database File** menu, select **Open**.
   d. For the key database type, select **JKS**.
   e. Type the keystore file name: testadmin.jks
   f. Type the location: ISDI_HOME/timsol/serverapi
   g. Enter the password when prompted. The default password is **administrator**.
   h. Click **Signer Certificates** in the drop-down menu and click **Add**.
   i. Use **Browse** to select the downloaded or exported DigiCert Global Root G2 certificate. Click **OK** to continue. The certificate is added in the certificate store.

5. Restart the Dispatcher service.

Importing the adapter profile

You can import a profile definition file, which creates a service type in IBM Security Verify Governance Identity Manager server. Use this option for importing adapter profiles.

Before you begin

- The IBM Security Verify Governance Identity Manager server is installed and running.
- You have root or administrator authority on the IBM Security Verify Governance Identity Manager server.
- The file to be imported must be a Java™ archive (JAR) file. The <Adapter>Profile.jar file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files. The JAR file for IBM Security Verify Governance Identity Manager is inside "Identity Manager" directory of the installation package.

About this task

Service definition files are also called adapter profile files.

If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a service with the adapter profile or open an account on the service. You must import the adapter profile again.

There are three adapter profiles included in the Workday HR Feed Adapter distribution package:

- IdentityManager\BPPerson\WorkdayHRProfile.jar
- IdentityManager\Person\WorkdayHRProfile.jar
- ISVG\WorkdayHRProfile.jar

If Business Partner entity is in scope then IdentityManager\BPPerson\WorkdayHRProfile.jar should be used in IBM Security Verify Governance Identity Manager instance else IdentityManager\Person\WorkdayHRProfile.jar should be used.

Note: It is not possible for both IdentityManager\BPPerson\WorkdayHRProfile.jar and IdentityManager\Person\WorkdayHRProfile.jar profiles to exist in the same IBM Security Verify Governance Identity Manager instance.

Note: ISVG\WorkdayHRProfile.jar profile is for IBM Security Verify Governance only and should not be used with IBM Security Verify Governance Identity Manager.

Procedure

1. Log on to the IBM Security Verify Governance Identity Manager server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.
   The Manage Service Types page is displayed.
3. On the Manage Service Types page, click **Import**.
   The Import Service Type page is displayed.
4. On the Import Service Type page, complete these steps:
   a. In the **Service Definition File** field, type the directory location of the <Adapter>Profile.jar file, or click **Browse** to locate the file.
   b. Click **OK** to import the file.

Results

A message indicates that you successfully submitted a request to import a service type.

What to do next

The import occurs asynchronously, which means it might take some time for the service type to load into the IBM Security Verify Governance Identity Manager server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is Failed, check the log files to determine why the import failed.

If you receive a schema-related error, see the trace.log file for information about it. The trace.log file location is specified by the **handler.file.fileDir** property that is defined in the enRoleLogging.properties file present in the IBM Security Verify Governance Identity Manager HOME\data directory.

Creating an adapter service/target

After you import the adapter profile on the IBM Verify Governance Identity Manager server, add a connector so that IBM Security Verify Governance Identity Manager server can communicate with the managed resource.

Before you begin

Complete Importing the adapter profile tasks.

About this task

To create or change a service, you must use the service/target form details to provide information for the service. Service forms might vary depending on the adapter. The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

To add a connector, complete these steps.

1. Log in to the IBM Security Verify Governance Identity Manager.
2. From the navigation tree, click **Manage Services**.
   Select a Service page is displayed.
3. On the Select a Service page, click **Create**.
   The Create a Service wizard is displayed.
4. On the Select the Type of Service page, click **Search** to locate a business unit.
   The Business Unit page is displayed.
5. On the Business Unit page, complete these steps:
   a. Type information about the business unit in the **Search information** field.
   b. Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.
      If the table contains multiple pages, you can do the following tasks:
      i. Click the arrow to go to the next page.
      ii. Type the number of the page that you want to view and click **Go**.
   c. In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
      Select the Type of Service page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
6. On the Select the Type of Service page, select a service type, and then click **Next**.
   If the table contains multiple pages, you can do the following tasks:
   a. Click the arrow to go to the next page.
   b. Type the number of the page that you want to view and click **Go**.
7. Specify appropriate values for all required fields on the service form under different tabs and click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

If the connection fails, contact the support who is responsible to manage the target resource.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

Service/Target Form details

Complete the service/target form fields.

The Workday HR Feed Adapter service form has several tabs:

- Connector Profile tab
- Connection tab
- Dispatcher Attributes tab
- Service Status tab

Connection Profile Tab

This tab provides information about the adapter service details.

Security Directory Integrator location

Specify the URL for the IBM Security Directory Integrator instance. The valid syntax for the URL is rmi://ipaddress:port/ITDIDispatcher, where ip-address is the IBM Security Directory Integrator host and port is the port number for the Dispatcher.

The default URL is rmi://localhost:1099/ITDIDispatcher. For information about changing the port number, see the IBM Security Dispatcher Installation and Configuration Guide.

Workday API Base URL

Specify the base API URL for the Workday Target. The valid syntax for the URL is: https://****-impl-services**.workday.com. (For example: https://wd2-impl-services1.workday.com)

Workday Tenant ID

Specify the tenant if for the API connection. Tenant ID can be identified based on below URL format.

https://wd2-impl-services1.workday.com/ccx/service/<Tenant_ID>/Human_Resources

Where *<Tenant_ID>* placeholder contains actual Workday tenant ID.

Exclude Inactive Workers

Select this option to exclude Inactive Workers from the reconciliation.

Exclude Employees

Select this option to exclude Employees from the reconciliation.

Exclude Contingent Workers

Select this option to exclude Contingent Workers from the reconciliation.

Exclude Inactive Locations

Select this option to exclude Inactive Locations from the reconciliation.

Exclude Inactive Job Families

Select this option to exclude Inactive Job Families from the reconciliation.

Workday API Page size

Optional: Provide pagination size between 1 to 999 for the Workday SOAP APIs. If no value is specified, page size will be defaulted 100.

Enable debug mode

Enable this attribute if additional logs need to be captured during the debug mode.

Soap API Version

Specify the Workday SOAP API version to be used. For example: v40.0
Note: Consult the release notes for the SOAP API versions that are supported for the installed adapter.

Person profile name

This is a read only field which contains the value **WorkdayHRPerson**.
It specifies that all the Workers from the Workday target will be created as **WorkdayHRPerson** in IBM Security Verify Governance Identity Manager.

Use workflow

If this checkbox is checked, then an identity policy needs to be created for the IBM Security Governance Identity Manager account for the new person. The Use workflow checkbox is checked by default.

Evaluate separation of duty policy when workflow is used

Select this option if evaluation of separation of duty policy is required when the workflow is used.

Placement rule

Provide the details for a placement rule. If unspecified, the default organization is used.
See Placement of the Person.

Connection tab

Workday Authentication Type

Select any one authentication type for SOAP API requests from the given list:

- Basic Authentication
- OAuth using JWT
- OAuth using Refresh Token
- X509 Authentication
- SAML Authentication

Note: Ensure to complete Workday SOAP API Authentication and Authorization setup before using this service

Workday User ID

Specify the Workday User Account created for the adapter. (For example: IBM_HR_Adapter_User)
This attribute is not required for OAuth using Refresh Token authentication type.

Workday User password

Specify the password for the Workday User Account created for the adapter. This attribute is required only for Basic Authentication.

Workday Keystore Path

Specify path to the Keystore located on the IBM Security Directory Integrator Server where Dispatcher service is running. It is required for OAuth using JWT, X509 and SAML authentication types.

Workday Keystore Type

Select type of Keystore (JKS or PKCS12). It is required for OAuth using JWT, X509 and SAML authentication types.

Workday Keystore Password

Specify the password for the Keystore. It is required for OAuth using JWT, X509 and SAML authentication types.

Workday Certificate Alias

Specify the Certificate Alias. It is required for OAuth using JWT, X509 and SAML authentication types.

Workday Certificate Password

Specify the Certificate password. It is required for OAuth using JWT, X509 and SAML authentication types.

Workday Client ID

Specify the Client ID of API Client created for the adapter. It is required for OAuth using JWT and Refresh Token authentication types.

Workday Client Secret

Specify the Client Secret generated during API Client Registration for the adapter. It is required only for OAuth using Refresh Token.

Workday Refresh Token

Specify the Refresh Token generated during API Client Registration for the adapter. It is required only for OAuth using Refresh Token.

Workday Certificate Common Name

Specify the common name of the certificate. It is required only for SAML authentication type. (For example: CN=ABC, OU=ABC, O=COMPANY, L=Austin, ST=Texas, C=US)

Workday Issuer ID

Specify the Issuer ID configured during the authentication setup for the adapter. It is required only for SAML authentication type.

Workday API Token Expiry in Seconds

Optional: Specify the Token Expiry Time in Seconds. By default, the value is set to 3600 seconds for SAML authentication type and 360 seconds for OAuth using JWT authentication type.

Note: For OAuth using JWT authentication type, Token Expiry cannot exceed 360 seconds as the Workday target responds with error when the value exceeds.

Dispatcher Attributes tab

This tab describes the Dispatcher attributes.

Note: If the following fields on the service form are changed for an existing service, restart the adapter service on the IBM Security Directory Integrator server.

- AL FileSystem path
- Max Connection Count

AL FileSystem Path

Specify the file path from where the Dispatcher loads the assembly lines. If you do not specify a file path, the Dispatcher loads the assembly lines that are received from IBM Security Verify Governance.

For example:

Windows operating system

C:\Program Files\IBM\TDI\V7.2\profiles

UNIX and Linux® operating system

/opt/IBM/TDI/V7.2/profiles

Max Connection Count

Specify the maximum number of assembly lines that the Dispatcher can execute simultaneously for the service.

For example, enter 10 if you want the Dispatcher to execute a maximum of 10 assembly lines simultaneously for the service. If you enter 0, the Dispatcher does not limit the number of assembly lines that are executed simultaneously for the service.

Assembly lines occupy the JVM memory. Too many assembly lines can cause an out-of-memory scenario in the IBM Security Directory Integrator server. Each assembly line also creates multiple connections to the end point. The end point might have a limit on the number of remote connections allowed. As such, the adapter requests might fail.

Disable Assembly Line Caching

Select the check box to disable the assembly line caching in the Dispatcher for the service. When disabled, the assembly lines for the Add, Modify, Delete, and Test operations are not cached.

Unselect the check box if the requirement is to enable caching. When enabled, the entire assembly line object is saved in the cache. The connection to the Workday resource is maintained. The next request that the adapter receives can reuse this connection.

Creating a new connection to the Workday resource can take a lot of time. Caching data can save time and resource utilization.

Service Status tab

Contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click Test Connection to populate the fields.

Last status update

Specifies the most recent datetime when the Status and information tab was updated.

Managed resource status

Specifies the status of the managed resource to which the adapter is connected.

Managed resource status message

Specifies the message (if any) returned by managed resource to which the adapter is connected.

Managed resource version

Specifies the version (if any) returned by managed resource to which the adapter is connected.

Profile version

Specifies the version of the profile that is installed for Workday HR Feed Adapter.

Adapter version

Specifies the version of the adapter that the service uses to provision request to the managed resource.

Adapter Connector version

Specifies the version of the Workday Connector used to connect to managed resource.

TDI version

Specifies the version of the IBM Security Directory Integrator on which the adapter is deployed.

Dispatcher version

Specifies the version of the Dispatcher.

Installation platform

Specifies summary information about the operating system where the adapter is installed.

Adapter account

Specifies the account that is running the adapter binary file.

Adapter up time

Specifies the datetime when the adapter started.

Adapter memory usage

Specifies the memory usage for running the adapter.

Verifying that the adapter is working correctly

After you install and configure the adapter, verify that the installation and configuration are correct.

Procedure

1. Test the connection for the service that you created on the IBM Security Verify Governance Identity Manager server.
2. Run a full reconciliation from the IBM Security Verify Governance Identity Manager server.
3. Verify the ibmdi.log file after each operation to ensure that no errors are reported.

Installing ILMT-Tags

This topic describes the procedures to install ILMT tag files.

Before you begin:

The Dispatcher must be installed.

Procedure:

Copy the files in the ILMT-Tags folder to the specified location:

- Windows:
  <SDI-HOME>\swidtag
- Unix/Linux:
  <SDI-HOME>/swidtag

Chapter 4. Upgrading

Upgrading an IBM® Security Directory Integrator-based adapter involves tasks such as upgrading the dispatcher, the connector, and the adapter profile.

See the Release Notes® for the supported software versions or for specific instructions.

Upgrading the Dispatcher

The new adapter package might require you to upgrade the Dispatcher.

Before you upgrade the Dispatcher, verify the version of the Dispatcher.

If the Dispatcher version that is mentioned in the release notes is later than the existing version on your workstation, install the Dispatcher.

If the Dispatcher version that is mentioned in the release notes is the same or earlier than the existing version, do not install the Dispatcher.

Note: The Dispatcher installer stops the Dispatcher service before the upgrade and restarts it after the upgrade is complete.

Upgrading the Connector

To upgrade the connector, replace existing binaries and connector. See Installing the adapter binaries or connector.

Upgrading the Adapter Profile

Steps for upgrading the adapter profile.

About this task

Read the adapter Release Notes for any specific instructions before you import a new adapter profile.

Note: Restart the Dispatcher service after importing the profile. Restarting the Dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.

There are three adapter profiles included in the Workday HR Feed Adapter distribution package:

- IdentityManager\BPPerson\WorkdayHRProfile.jar
- IdentityManager\Person\WorkdayHRProfile.jar
- ISVG\WorkdayHRProfile.jar

If Business Partner entity is in scope then IdentityManager\BPPerson\WorkdayHRProfile.jar should be used in IBM Security Verify Governance Identity Manager instance else IdentityManager\Person\WorkdayHRProfile.jar should be used.

Note: It is not possible for both IdentityManager\BPPerson\WorkdayHRProfile.jar and IdentityManager\Person\WorkdayHRProfile.jar profiles to exist in the same IBM Security Verify Governance Identity Manager instance.

Note: ISVG\WorkdayHRProfile.jar profile is for IBM Security Verify Governance only and should not be used with IBM Security Verify Governance Identity Manager.

Chapter 5. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

See the IBM Security Dispatcher Installation and Configuration Guide for the following configuration options:

- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

Enabling TLS 1.2 in IBM Security Directory Integrator

Perform the steps in this topic to enable TLS v1.2 in IBM® Security Directory Integrator.

Procedure

1. Apply the recommended fix packs and limited availability (LA) versions on Security Directory Integrator. See Recommended fixes for IBM Security Directory Integrator (SDI).
2. After applying the appropriate updates, modify the <SOLUTION_DIRECTORY>/solution.properties file by appending the following text to the bottom of the file:

```
## ----------------------------------------------------------------------------------------------------

## Protocols to enforce SSL protocols in a SDI Server

## Optional values for com.ibm.di.SSL* property (TLSv1, TLSv1.1, TLSv1.2).

## This can be a multi-valued comma separated property

## Optional values for com.ibm.jsse2.overrideDefaultProtocol property (SSL_TLSv2,TLSv1,TLSv11,TLSv12).

## This is a single value property.

## ----------------------------------------------------------------------------------------------------

com.ibm.di.SSLProtocols=TLSv1.1,TLSv1.2

com.ibm.di.SSLServerProtocols=TLSv1.1,TLSv1.2

com.ibm.jsse2.overrideDefaultProtocol=TLSv12

com.ibm.jsse2.overrideDefaultTLS=true
```

3. Restart the Dispatcher service and try connecting to the tenants that are using TLS v1.2.

Chapter 6. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?

- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you use the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being done?
- Is a certain sequence of events required for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might occur around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Error messages and problem solving

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

Table 1 and Table 2 contain warnings or errors, which might be displayed when the Workday adapter is installed on your system.

Table 1. Specific messages and actions

Message number	Message	Action
CTGIMT600E	An error occurred while establishing communication with the IBM Security Directory Integrator server.	• Verify that the IBM Security Directory Integrator- based adapter service is running. • Verify that the URL specified on the service form for IBM Security Directory Integrator is correct.
CTGIMT001E	The following error occurred. Error during authentication. Ensure Client ID, Client Secret, and the Workday base URL is correct	• Verify that the Workday server URL is running. • Verify that the Workday client ID and client secret that is specified on the service form of the Workday are correct.

CTGIMU107W	The following error occured: Test Connection Fails: The connection to the specified service cannot be established.	Verify the service information and try again. ibmdi.log The service name might contain special characters that IBM Security Directory Integrator cannot handle. For example, “/”.

Table 2. General messages and actions

Message	Action
Adapter profile is not displayed in the user interface after installing the profile.	You must stop and restart the Security Directory Integrator server or wait until the cache times out (up to 10 minutes) for IBM Security Verify Governance to refresh the list of attribute names.

Enabling DEBUG Logs on SDI Server

About this task

This task is required to enable Debug logs on SDI Server to generate additional logs required to help in the analysis of any issue reported against this adapter.

Procedure

1. Stop the SDI Server process.

   Pre-7.2.0-ISS-SDI-FP0008

   a. Edit the <SDI_Solution_Directory>/etc/log4j.propertiesfile.

   b. Modify the following line: log4j.rootCategory=INFO, Default to log4j.rootCategory=DEBUG, Default

   Post-7.2.0-ISS-SDI-FP0008

   a. Edit the <SDI_Solution_Directory>/etc/log4j2.xml file.

   b. Modify the following line: <Root level="info"> to <Root level="debug">

2. Start the SDI Server process.
3. Re-create the issue and collect the <SDI_Solution_Dir>/logs/ibmdi.log file.

Intermittently connector stops generating logs in SDI 7.2.0.11 onwards

About this task

This task is only for SDI 7.2.0.11 onwards.

Procedure

1. Stop the SDI Server process.
2. Edit the <SDI_Solution_Directory>/etc/global.properties.
3. Add following lines to the end of file

   ```
   #----------------------------------
   #Logging close property
   #----------------------------------
   com.ibm.di.logging.close=false
   ```

4. Start the SDI Server process.

Chapter 7. Uninstalling

To remove an adapter from the IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server for any reason, you must remove all the components that were added during installation. Uninstalling a Workday HR Feed Adapter mainly involves removing the Service/Target, adapter profile from the IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server and connector file and any other libraries deployed as a part of adapter installation from IBM Security Directory Integrator Server. Depending on the adapter, some of these tasks might not be applicable, or there can be other tasks.

If the server is offline, the completed adapter requests might not be recovered when the server is back online.

Deleting the adapter profile

Remove the adapter service/target type from the IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server. Before you delete the adapter profile, ensure that no objects exist on the IBM Security Verify Governance Identity Manager or IBM Security Verify Governance server that reference the adapter profile.

Note: The Dispatcher component must be installed on your system for adapters to function correctly in a Security Directory Integrator environment. When you delete the adapter profile, do not uninstall the Dispatcher.

For specific information about how to delete the adapter profile, see the IBM Security Verify Governance product documentation.

Chapter 8. Reference

Reference information is organized to help you locate particular facts quickly, such as adapter attributes, registry settings, and environment variables.

Adapter attributes and object classes

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

The Workday HR Feed Adapter supports a standard set of attributes.

Table 1. Supported Person/Account attributes - erworkdayhraccount

Workday HR Feed Adapter attribute name	Description	Required	Managed Resource Attribute
erworkdayhrworkerwid	Worker WID	YES	Worker/Worker_Reference/ID[@type='WID']
erworkdayhrworkertype	Worker Type	NO	Employee if reponse contains Worker/Worker_Reference/ID[@type='Employee_ID'] else Contingent Worker if response contains Worker/Worker_Reference/ID[@type='Contingent_Worker_ID']
erworkdayhrworkerid	Worker ID	YES	Worker/Worker_Data/Worker_ID
erworkdayhruserid	Username	NO	Worker/Worker_Data/User_ID
erworkdayhruniversalid	Universal ID	NO	Worker/Worker_Data/Universal_ID
erworkdayhrfirstnamelegal	Legal First Name	NO	Worker/Worker_Data/Personal_Data/Name_Data/Legal_Name_Data/Name_Detail_Data/First_Name
erworkdayhrmiddlenamelegal	Legal Middle Name	NO	Worker/Worker_Data/Personal_Data/Name_Data/Legal_Name_Data/Name_Detail_Data/Middle_Name
erworkdayhrlastnamelegal	Legal Last Name	NO	Worker/Worker_Data/Personal_Data/Name_Data/Legal_Name_Data/Name_Detail_Data/Last_Name
erworkdayhrfirstnamepreferred	Preferred First Name	NO	Worker/Worker_Data/Personal_Data/Name_Data/Preferred_Name_Data/Name_Detail_Data/First_Name
erworkdayhrmiddlenamepreferred	Preferred Middle Name	NO	Worker/Worker_Data/Personal_Data/Name_Data/Preferred_Name_Data/Name_Detail_Data/Middle_Name
erworkdayhrlastnamepreferred	Preferred Last Name	NO	Worker/Worker_Data/Personal_Data/Name_Data/Preferred_Name_Data/Name_Detail_Data/Last_Name

erworkdayhrbirthdate	Date of Birth (yyyyMMdd)	NO	Worker/Worker_Data/Personal_Data/Personal_Information_Data/Birth_Date
erworkdayhrbirthcountrycode	Country of Birth place	NO	Worker/Worker_Data/Personal_Data/Personal_Information_Data/Country_of_Birth_Reference/ID[@type='ISO_3166-1_Alpha-3_Code']
erworkdayhrbirthregion	Region of birth place	NO	Worker/Worker_Data/Personal_Data/Personal_Information_Data/Region_of_Birth_Descriptor
erworkdayhrbirthcity	City of birth place	NO	Worker/Worker_Data/Personal_Data/Personal_Information_Data/City_Of_Birth
erworkdayhrworkphonecode	International phone code number	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Phone_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID']='WORK']/International_Phone_Code
erworkdayhrworkphonenumber	Phone number	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Phone_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID']='WORK']/Phone_Number
erworkdayhrworkemailaddress	Email address	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Email_Address_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID']='WORK']/Email_Address
erworkdayhrpositioneffectivedate	Effective date for position (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data[@Effective_Date]
erworkdayhrpositionid	Position ID	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Position_ID
erworkdayhrpositiontitle	Position Title	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Position_Title
erworkdayhrbusinesstitle	Business Title	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Business_Title
erworkdayhrpositionstartdate	Position start date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Start_Date
erworkdayhremploymentenddate	Employement end date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/End_Employment_Date

erworkdayhrpositionworkertype	Worker type for the position	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Worker_Type_Reference/ID[@type='Employee_Type_ID'] or Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Worker_Type_Reference/ID[@type='Contingent_worker_Type_ID']
erworkdayhrtimeinposition	Position Time Type	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Position_Time_Type_Reference/ID[@type='Position_Time_Type_ID']
erworkdayhrjobclassificationrefid	Job Classification Reference ID	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Job_Classification_Summary_Data/Job_Classification_Reference/ID[@type='Job_Classification_Reference_ID']
erworkdayhrjobprofilerefid	Job profile reference ID	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Job_Profile_Summary_Data/Job_Profile_Reference/ID[@type='Job_Profile_ID']
erworkdayhrjobcategoryrefid	Job Category Reference ID	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Job_Profile_Summary_Data/Job_Category_Reference/ID[@type='Job_Category_ID']
erworkdayhrjobfamilyrefid	Job Family Reference ID	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Job_Profile_Summary_Data/Job_Family_Reference/ID[@type='Job_Family_ID']
erworkdayhrjobfamilygroupid	Job Family Group ID	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Job_Profile_Summary_Data/Job_Family_Reference/ID[@type='Job_Family_Group_ID']
erworkdayhrjobprofilename	Job profile name	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Job_Profile_Summary_Data/Job_Profile_Name
erworkdayhrjoblocationid	Job Location	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Business_Site_Summary_Data/Location_Reference/ID[@type='Location_ID']
erworkdayhrworkspacerefid	Workspace reference ID	NO	Worker/Worker_Data/Employment_Data/Worker_Job_Data/Position_Data/Work_Space__Reference[@type='Location_ID']
erworkdayhrworkeractivestatus	Worker active status	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Active
erworkdayhractivestatusdate	Most recent active status date	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Active_Status_Date

	(yyyyMMdd)		
erworkdayhrhiredate	Hire date or contract start date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Hire_Date
erworkdayhroriginalhiredate	Earliest hire date for the worker (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Original_Hire_date
erworkdayhrretired	Retired status	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Retired
erworkdayhrretirementdate	Most recent Retirement Date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Retirement_Date
erworkdayhrterminated	Termination status	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Terminated
erworkdayhrterminationdate	Most recent Termination Date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Termination_Date
erworkdayhrresignationdate	Resignation submission date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Resignation_Date
erworkdayhrexpecteddateofreturn	Canadian worker expected date of return(Specific to Canadian employe	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Expected_Date_of_Return

	ment) (yyyyMMdd)		
erworkdayhrnotreturning	Is Canadian worker not expected to return(Specific to Canadian employement)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Not_Returning
erworkdayhrprobationstartdate	Probation start date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Probation_Start_Date
erworkdayhrprobationenddate	Probation end date (yyyyMMdd)	NO	Worker/Worker_Data/Employment_Data/Worker_Status_Data/Probation_End_Date
erworkdayhrusername	Worker Account Username	NO	Worker/Worker_Data/User_Account_Data/User_Name
erworkdayhrpreferredlangid	Preferred language for user account	NO	Worker/Worker_Data/User_Account_Data/User_Language__Reference/ID[@type='User_Language_ID']
erworkdayhrpreferredcommlangid	Preferred communication language	NO	Worker/Worker_Data/User_Account_Data/Preferred_Communication_Language_Reference/ID[@type='User_Language_ID']
erworkdayhrprovisioninggroupandstatus	Latest status of the provisioning group assignment :	NO	Concatenation of Worker/Worker_Data/Account_Provisioning_Data/Provisiong_group and Worker/Worker_Data/Account_Provisioning_Data/Status separated by pipe (|)

	ProvisioningGroup|Status		
erworkdayhrorganizationroles	Organization Roles (Organization_ID|Role_ID)	NO	Concatenation of Organization/Organization_Data/Reference_ID and Organization/Organization_Data/Roles_Data/Organization_Role_Data/Role_Reference/ID[@type='Organization_Role_ID'] separated by pipe (|)
erworkdayhrorganizationmembership	Organization Membership	NO	Worker/Worker_Data/Organization_Data/Worker_Organization_Data/Organization_Reference/ID[@type='Organization_Reference_ID']
erworkdayhrsupervisoryorgmanagerid	Supervisory Organization Manager ID	NO	Worker/Worker_Data/Management_Chain_Data/Worker_Supervisory_Management_Chain_Data/Management_Chain_Data[last()]/Manager_Reference/ID[@type='Employee_ID'] or Worker/Worker_Data/Management_Chain_Data/Worker_Supervisory_Management_Chain_Data/Management_Chain_Data[last()]/Manager_Reference/ID[@type='Contingent_Worker_ID']
erworkdayhrgendercode	Gender Identity	NO	Worker/Worker_Data/Personal_Data/Personal_Information_Data/Gender_Identity_Reference/ID[@type='Gender_Identity_ID']
erworkdayhrworkaddressline1	Work Address Line 1	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Address_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID'] ='WORK']/Address_Line_Data[@type='ADDRESS_LINE_1']
erworkdayhrworkaddresscity	Work City	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Address_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID'] ='WORK']/Municipality
erworkdayhrworkaddressstate	Work Address State	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Address_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID'] ='WORK']/Country_Region_Descriptor
erworkdayhrworkaddresscountry	Work Address Country	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Address_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID'] ='WORK']/Country_Reference/ID[@type='ISO_3166-1_Alpha-3_Code']
erworkdayhrworkaddresspostalcode	Work Address Postal Code	NO	Worker/Worker_Data/Personal_Data/Contact_Data/Address_Data[Usage_Data[@Public='true']/Type_Data[@Primary='true']/Type_Reference/ID[@type='Communication_Usage_Type_ID'] ='WORK']/Postal_Code

Table 2. Supported Organization attributes - erworkdayhrorganization

Workday HR Feed Adapter attribute name	**Description**	**Required**	**Managed Resource Attribute**
erworkdayhrorgrefid	Organization ID	YES	Organization/Organization_Data/Reference_ID
erworkdayhrorgname	Organization Name	NO	Organization/Organization_Data/Name
erworkdayhrorgdesc	Organization Description	NO	Organization/Organization_Data/Description
erworkdayhrorgcode	Organization Code	NO	Organization/Organization_Data/Organization_Code
erworkdayhrorgtyperefid	Organization Type Reference ID	NO	Organization/Organization_Data/Organization_Type_Reference/ID[@type='Organization_Type_ID']
erworkdayhrorgsubtyperefid	Organization Sub Type Reference ID	NO	Organization/Organization_Data/Organization_Subtype_Reference/ID[@type='Organization_Subtype_ID']
erworkdayhrorgavailibilitydate	Organization Availability Date	NO	Organization/Organization_Data/Availibility_Date
erworkdayhrorglastupdateddatetime	Organization Last Updated DateTime	NO	Organization/Organization_Data/Last_Updated_DateTime
erworkdayhrorginactive	Organization inactive status	NO	Organization/Organization_Data/Inactive
erworkdayhrorginactivedate	Organization	NO	Organization/Organization_Data/Inactive_Date

	inactive date		
erworkdayhrorgmanagerrefid	Organization Manager Reference ID	NO	Organization/Organization_Data/Manager_Reference/ID[@type='Employee_ID']
erworkdayhrorgleadershiprefid	Organization Leadership Reference IDs	NO	Organization/Organization_Data/Leadership_Reference/ID[@type='Employee_ID']
erworkdayhrorgownerrefid	Organization Owner Reference ID	NO	Organization/Organization_Data/Organization_Owner_Reference/ID[@type='Employee_ID']
erworkdayhrorgexternalurl	Organizational External URL	NO	Organization/Organization_Data/External_URL_Reference/ID[@type='URL']
erworkdayhrorgrolerefid	Organization Roles	NO	Organization/Organization_Data/Roles_Data/Organization_Role_Data/Role_Reference/ID[@type='Organization_Role_ID']
erworkdayhrorgtoplevelorgrefid	Top-level Organization	NO	Organization/Organization_Data/Hierarchy_Data/Top-Level_Organization_Reference/ID[@type='Organization_Reference_ID']
erworkdayhrorgsuperiororgrefid	Superior Organization	NO	Organization/Organization_Data/Hierarchy_Data/Superior_Organization_Reference/ID[@type='Organization_Reference_ID']
erworkdayhrorgsubordinateorgrefid	Subordinate Organizations	NO	Organization/Organization_Data/Hierarchy_Data/Subordinate_Organization_Reference/ID[@type='Organization_Reference_ID']
erworkdayhrorgincludedorgrefid	Member Organizations	NO	Organization/Organization_Data/Hierarchy_Data/Included_Organization_Reference/ID[@type='Organization_Reference_ID']
erworkdayhrorgincludedinorgrefid	Member of Organizations	NO	Organization/Organization_Data/Hierarchy_Data/Included_In_Organization_Reference/ID[@type='Organization_Reference_ID']

erworkdayhrorgstaffingmodel	Staffing model for organization	NO	Organization/Organization_Data/Supervisory_Data/Staffing_Model
erworkdayhrorglocationrefid	Primary Location Reference ID	NO	Organization/Organization_Data/Supervisory_Data/Location_Reference/ID[@type='Location_ID']
erworkdayhrorgavailableforhire	Is organization available for hire	NO	Organization/Organization_Data/Supervisory_Data/Available_For_Hire
erworkdayhrorghiringfreeze	Is Hiring Freeze currently in effect	NO	Organization/Organization_Data/Supervisory_Data/Hiring_Freeze

Table 3. Supported Location attributes - erworkdayhrlocation

Workday HR Feed Adapter attribute name	**Description**	**Required**	**Managed Resource Attribute**
erworkdayhrlocid	Location ID	YES	Location/Location_Data/Location_ID
erworkdayhrloceffectivedate	Location Effective Date	NO	Location/Location_Data/Effective_Date
erworkdayhrlocname	Location Name	NO	Location/Location_Data/Location_Name
erworkdayhrlocusagerefid	Location Usage Reference ID	NO	Location/Location_Data/Location_Usage_Reference/ID[@type='Location_Usage_ID']
erworkdayhrloctyperefid	Location Usage Reference ID	NO	Location/Location_Data/Location_Type_Reference/ID[@type='Location_Type_ID']

erworkdayhrlocsuperiorlocrefid	Superior Location Reference ID	NO	Location/Location_Data/Superior_Location_Reference/ID[@type='Location_ID']
erworkdayhrlocinactive	Is location inactive	NO	Location/Location_Data/Inactive
erworkdayhrloctimeprofilerefid	Time Profile Reference ID	NO	Location/Location_Data/Time_Profile_Reference/ID[@type='Time_Profile_ID']
erworkdayhrloclocalerefid	Locale Reference ID	NO	Location/Location_Data/Locale_Reference/ID[@type='Locale_ID']
erworkdayhrlocdisplaylangrefid	Display Language Rereferce ID	NO	Location/Location_Data/Display_Language_Reference/ID[@type='User_Language_ID']
erworkdayhrloctimezonerefid	Time Zone Reference ID	NO	Location/Location_Data/Time_Zone_Reference/ID[@type='Time_Zone_ID']
erworkdayhrlocdefaultcurrencyrefid	Default Currency Reference ID	NO	Location/Location_Data/Default_Currency_Reference/ID[@type='Currency_ID']
erworkdayhrlocexternalname	External Name	NO	Location/Location_Data/External_Name
erworkdayhrloctradename	Trade Name	NO	Location/Location_Data/Trade_Name
erworkdayhrlocworksiteidcode	Worksite ID Code	NO	Location/Location_Data/Worksite_ID_Code
erworkdayhrlocidentifier	Location Identifier	NO	Location/Location_Data/Location_Identifier
erworkdayhrlocaddresseffectivedate	Effective date of address	NO	Location/Location_Data/Contact_Data/Address_Data/Country_Reference/ID[@type='ISO_3166-1_Alpha-3_Code']
erworkdayhrlocaddresscountrycode	Country code	NO	Location/Location_Data/Contact_Data/Address_Data/Address_Line_Data[@type='ADDRESS_LINE_1']

erworkdayhrlocaddressline1	Address Line 1	NO	Location/Location_Data/Contact_Data/Address_Data/Address_Line_Data[@type='ADDRESS_LINE_2']
erworkdayhrlocaddressline2	Address Line 2	NO	Location/Location_Data/Contact_Data/Address_Data/Municipality
erworkdayhrlocmunicipality	City	NO	Location/Location_Data/Contact_Data/Address_Data/Country_Region_Descriptor
erworkdayhrloccountryregion	State/Province	NO	Location/Location_Data/Contact_Data/Address_Data/Postal_Code
erworkdayhrlocpostalcode	Postal code	NO	Location/Location_Data/Contact_Data/Address_Data/Address_ID
erworkdayhrlocinternationalphonecode	International phone code number	NO	Location/Location_Data/Contact_Data/Phone_Data/International_Phone_Code
erworkdayhrlocphonenumber	Full phone number	NO	Location/Location_Data/Contact_Data/Phone_Data/Phone_Number
erworkdayhrlocemailaddress	Email Address	NO	Location/Location_Data/Contact_Data/Email_Address_Data/Email_Address
erworkdayhrlochierarchyrefid	Location Hierarchy Reference ID	NO	Location/Location_Data/Location_Hierarchy_Reference/ID[@type='Organization_Reference_ID']

Table 4. Supported Job Profile attributes - erworkdayhrjobprofile

Workday HR Feed Adapter attribute name	**Description**	**Required**	**Managed Resource Attribute**
erworkdayhrjobcode	Job Code	YES	Job_Profile/Job_Profile_Data/Job_Code
erworkdayhrjobtitle	Job Title	NO	Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Job_Title
erworkdayhrjobprofileprivatetitle	Job Profile Private Title	NO	Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Job_Profile_Private_Title
erworkdayhrjobcategoryrefid	Job Category Reference ID	NO	Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Job_Category_Reference/ID[@type='Job_Category_ID']
erworkdayhrjoblevelrefid	Job Level	NO	Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Job_Level_Reference/ID[@type='Job_Level_ID']

	Reference ID		
erworkdayhrjobfamilyrefid	Job Family Reference ID	NO	Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Job_Family_Data/Job_Family_Reference/ID[@type='Job_Family_ID']
erworkdayhrjobclassificationrefid	Job Classification Reference ID	NO	Job_Profile/Job_Profile_Data/Job_Classification_Data/Job_Classification_Reference/ID[@type='Job_Classification_Reference_ID']
erworkdayhrjobeffectivedate	Effective Date of the Job Profile	NO	Job_Profile/Job_Profile_Data/Effective_Date
Erworkdayhrjobinactive	Job Inactive Status	NO	Job_Profile/Job_Profile_Data/Job_Profile_Basic_Data/Inactive

Table 5. Supported Job Family attributes - erworkdayhrjobfamily			
Workday HR Feed Adapter attribute name	**Description**	**Required**	**Managed Resource Attribute**
erworkdayhrjobfamilyid	Job Family ID	YES	Job_Family/Job_Family_Data/ID
erworkdayhrjobfamilyname	Job Family Name	NO	Job_Family/Job_Family_Data/Name
erworkdayhrjobfamilysummary	Job Family Summary	NO	Job_Family/Job_Family_Data/Summary
erworkdayhrjobfamilyinactive	Job Family Inactive Status	NO	Job_Family/Job_Family_Data/Inactive
erworkdayhrjobfamilyeffectivedate	Effective date of Job Family	NO	Job_Family/Job_Family_Data/Effective_Date

Table 6. Supported Job Family Group attributes - erworkdayhrjobfamilygroup			
Workday HR Feed Adapter attribute name	**Description**	**Required**	**Managed Resource Attribute**
erworkdayhrjobfamilygroupid	Job Family Group ID	YES	Job_Family_Group/Job_Family_Group_Data/ID
erworkdayhrjobfamilygroupname	Job Family	NO	Job_Family_Group/Job_Family_Group_Data/Name

	Group Name		
erworkdayhrjobfamilygroupsummary	Job Family Group Summary	NO	Job_Family_Group/Job_Family_Group_Data/Summary
erworkdayhrjobfamilygroupinactive	Job Family Group Inactive Status	NO	Job_Family_Group/Job_Family_Group_Data/Inactive
erworkdayhrjobfamilygroupeffectivedate	Effective date of Job Family Group	NO	Job_Family_Group/Job_Family_Group_Data/Effective_Date

Table 7. Supported Job Category attributes - erworkdayhrjobcategory

Workday HR Feed Adapter attribute name	Description	Required	Managed Resource Attribute
erworkdayhrjobcategoryid	Job Categroy ID	YES	Job_Category/Job_Category_Data/Job_Category_ID
erworkdayhrjobcategoryname	Job Category Name	NO	Job_Category/Job_Category_Data/Job_Category_Name
erworkdayhrjobcategorydesc	Job Category Description	NO	Job_Category/Job_Category_Data/Job_Category_Description
erworkdayhrjobcategoryinactive	Job Category Inactive Status	NO	Job_Category/Job_Category_Data/Inactive

Table 8. Supported Job Classification attributes - erworkdayhrjobclassification

Workday HR Feed Adapter attribute name	Description	Required	Managed Resource Attribute
erworkdayhrjobclassificationrefid	Job Classification Reference ID	YES	Job_Classification_Group/Job_Classification_Group_Data/Job_Classification/Job_Classification_Data/ID

erworkdayhrjobclassificationid	Job Classification ID	NO	Job_Classification_Group/Job_Classification_Group_Data/Job_Classification/Job_Classification_Data/Job_Classification_ID
erworkdayhrjobclassificationdesc	Job Classification Description	NO	Job_Classification_Group/Job_Classification_Group_Data/Job_Classification/Job_Classification_Data/Description
erworkdayhrjobclassificationinactive	Job Classification Inactive Status	NO	Job_Classification_Group/Job_Classification_Group_Data/Job_Classification/Job_Classification_Data/Inactive
erworkdayhrjobclassificationgroupprefid	Job Classification Group reference ID	NO	Job_Classification_Group/Job_Classification_Group_Data/ID

Table 9. Supported Job Classification Group attributes - erworkdayhrjobclassificationgroup

Workday HR Feed Adapter attribute name	Description	Required	Managed Resource Attribute
erworkdayhrjobclassificationgroupprefid	Job Classification Group reference ID	YES	Job_Classification_Group/Job_Classification_Group_Data/ID
erworkdayhrjobclassificationgroupname	Job Classification Group Name	NO	Job_Classification_Group/Job_Classification_Group_Data/Job_Classification_Group_Name
erworkdayhrjobclassificationgroupeffectivedate	Effective date of Job Classification Group	NO	Job_Classification_Group/Job_Classification_Group_Data/Effective_Date
erworkdayhrjobclassificationgroupinactive	Job Classification Group Inactiv	NO	Job_Classification_Group/Job_Classification_Group_Data/Inactive

	e Status		

Table 10. Supported Gender Identity attributes - erworkdayhrgenderidentity

Workday HR Feed Adapter attribute name	Description	Required	Managed Resource Attribute
erworkdayhrgenderid	Gender Identity ID	YES	Gender_Identity/Gender_Identity_Data/ID
erworkdayhrgendercode	Gender Identity Code	NO	Gender_Identity/Gender_Identity_Data/Gender_Identity_Code
erworkdayhrgendername	Gender Identity Name	NO	Gender_Identity/Gender_Identity_Data/Gender_Identity_Name
erworkdayhrgenderdescription	Gender Identity Description	NO	Gender_Identity/Gender_Identity_Data/Gender_Identity_Inactive