IBM Security Identity Governance and Intelligence

PeopleSoft HR feed adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the IBM® Security Identity server. The PeopleSoft HR feed adapter enables communication between the IBM Security Identity server and the PeopleSoft server.

Features of the adapter

The adapter is designed to reconcile personal and organizational information from the target system.

It checks the connection between the PeopleSoft Application Server and IBM Security Identity Governance and Intelligence.

The adapter runs in agentless mode. It communicates to the target system by using the JDBC driver and the PeopleTools Java API.

Architecture

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

The adapter requires the following components:

- Dispatcher
- Security Directory Integrator connector
- IBM Security Identity Adapter profile

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

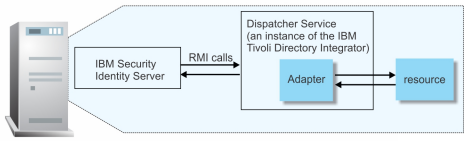

Figure 1. The architecture of the PeopleSoft HR feed adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

- The IBM Security Identity server
- The IBM Security Directory Integrator server
- The managed resource
- The 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 PeopleSoft Application Server:

- IBM Security Identity server
- Security Directory Integrator server

- PeopleSoft HR feed adapter

The PeopleSoft Application Server is installed on a different server as shown in Figure 2 on page 2.

Figure 2. Example of a single server configuration

Multiple server configuration

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

- IBM Security Identity server
- Security Directory Integrator server
- PeopleSoft HR feed adapter
- PeopleSoft Application Server

TheSecurity Directory Integrator server and the PeopleSoft HR feed adapter are installed on the same server as shown in Figure 3 on page 2.

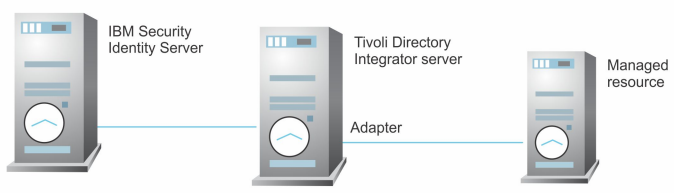

Figure 3. Example of a multiple server configuration

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.

Use the Preinstallation roadmap to prepare the environment.

Table 1. Preinstallation roadmap	
Task	**For more information, see**
Verify that your environment meets the software and hardware requirements for the adapter.	"Prerequisites" on page 10.
Obtain the installation software.	"Software downloads" on page 12.
Obtain the necessary information for the installation and configuration.	"Installation worksheet" on page 12.

Use the Installation and configuration roadmap to complete the actual installation and configuration of the adapter.

Table 2. Installation and configuration roadmap	
Task	**For more information, see**
Install the dispatcher.	"Installing the dispatcher" on page 17.
Install the connector.	"Installing the adapter binaries or connector" on page 19
Load the PeopleTools project in the IBM Security Identity Governance and Intelligence.	"Loading the project" on page 24
Import the adapter profile into the IBM Security Identity server.	Importing the adapter profile
Create an adapter service.	Creating an adapter service
Configure the adapter.	Chapter 6, "Configuring," on page 83

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 6.x

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. Install the dispatcher.

2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Create an adapter service/target.
8. Install the adapter language package.
9. Verify that the adapter is working correctly.

Upgrade

To upgrade the adapter, do a complete re-installation of the adapter. Follow the *Installation roadmap*.

Configuration

Complete these tasks.

1. Configure secure communication between the IBM Security Identity 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
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations

- Special attributes

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

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

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.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 7.x

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. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Create an adapter service/target.
8. Install the adapter language package.
9. Verify that the adapter is working correctly.

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 Identity 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
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 6.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

Software downloads

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

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.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager

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. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Create an adapter service/target.
8. Install the adapter language package.
9. Verify that the adapter is working correctly.

Upgrade

To upgrade the adapter, do a complete re-installation of the adapter. Follow the *Installation roadmap*.

Configuration

Complete these tasks.

1. Configure secure communication between the IBM Security Identity 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
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 6.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

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

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.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence

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

Note: There is a separate instruction for installing, upgrading or uninstalling adapters from the IBM Security Identity Governance and Intelligence virtual appliance.

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. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Load attribute mapping.
8. Set account defaults.
9. Create an adapter service/target.
10. Install the adapter language package.
11. Verify that the adapter is working correctly.

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 Identity 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
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

1. Stop the adapter service.
2. Remove the adapter binaries or connector.
3. Remove 3rd party client libraries.
4. Delete the adapter service/target.
5. Delete the adapter profile.

Reference

See the following topics.

- Adapter attributes and object classes
- Adapter attributes by operations
- Special attributes

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 6.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

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

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.

Prerequisites

Verify that your environment meets the software and hardware requirements for the adapter.

Table 3 on page 11 identifies the prerequisites for the adapter installation.

Table 3. Prerequisites to install the adapter	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
IBM Security Identity server	The following servers are supported: • IBM Security Identity Governance and Intelligence server Version 5.2.5
PeopleSoft Enterprise	Version 9.2
PeopleTools Software	Version 8.54 with HRMS module
Security Directory Integrator adapters solution directory	A Security Directory Integrator work 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.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 6.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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.

Software downloads

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

Go to IBM Passport Advantage. See the *IBM Security Identity Governance and Intelligence Download Document*.

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

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 6.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

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.

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 4. Required information to install the adapter

Required information	Description	Value
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	See the *Dispatcher Installation and Configuration Guide*.	**Windows:** *drive*`\Program Files\IBM\TDI\V7.2\`*timsol* **UNIX:** `/opt/IBM/TDI/V7.2/`*timsol*

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 6.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Manager 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

Prerequisites
Verify that your environment meets the software and hardware requirements for the adapter.

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

Chapter 3. Installing in the Security Identity Governance and Intelligence virtual appliance

For Security Identity Governance and Intelligence target management, you can install an IBM Security Identity Adapters or a custom adapter on the built-in Security Directory Integrator in the virtual appliance instead of installing the adapter externally. As such, there is no need to manage a separate virtual machine or system.

About this task

This procedure is applicable for a selected list of Identity Adapters. See the Identity Adapters product documentation at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm to determine which adapters are supported in Identity Governance and Intelligence, and which can be installed on the virtual appliance.

All Identity Governance and Intelligence supported adapters can be installed externally on the virtual appliance. Depending on the adapter, an external Security Directory Integrator may be required.

See the corresponding *Adapter Installation and Configuration Guide* for the specific prerequisites, installation and configuration tasks, and issues and limitations. See the *Adapters Release Notes* for any updates to these references.

Procedure

1. Download the adapter package from the IBM Passport Advantage.
   For example, `Adapter-<Adaptername>.zip`.

   The adapter package includes the following files:

Table 5. Adapter package contents

Files	Descriptions
`bundledefinition.json`	The adapter definition file. It specifies the content of the package, and the adapter installation and configuration properties that are required to install and update the adapter.
Adapter JAR profile	An Security Directory Integrator adapter always include a JAR profile which contains: • `targetProfile.json` – Service provider configuration – Resource type configuration – SCIM schema extensions – List of assembly lines • A set of assembly lines in XML files • A set of forms in XML files • Custom properties that include labels and messages for supported languages. Use the **Target Administration** module to import the target profile.

Table 5. Adapter package contents (continued)	
Files	**Descriptions**
Additional adapter specific files	Examples of adapter specific files: • Connector jar files • Configuration files • Script files • Properties files The file names are specified in the adapter definition file along with the destination directory in the virtual appliance.

2. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**.
3. Select the instance of the Security Directory Integrator for which you want to manage the adapters and click **Manage** > **SDI Adapters**

   The **SDI Adapters** window is displayed with a table that list the name, version, and any comments about the installed adapters.
4. On the **SDI Adapters** window, click **Install**.
5. On the **File Upload** window, click **Browse** to locate the adapter package and then click **OK**.
   For example, `Adapter-<Adaptername>.zip`.
6. Provide the missing 3rd party libraries when prompted.
   a) On the **File Upload** for Pre-requisite files window, click **Select Files**.

      A new **File Upload** window is displayed.

   b) Browse and select all the missing libraries. For example, `httpclient-4.0.1.jar`

   c) Click **Open**.

      The selected files are listed in the **File Upload** for Pre-requisite files window.

   d) Click **OK**.

      The missing files are uploaded and the adapter package is updated with the 3rd party libraries.
7. Enable secure communication.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Edit**.

   c) Click the **Enable SSL** check box.

   d) Click **Save Configuration**.
8. Import the SSL certificate to the IBM Security Directory Integrator server.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Manage** > **Certificates**.

   c) Click the **Signer** tab.

   d) Click **Import**.

      The **Import Certificate** window is displayed.

   e) Browse for the certificate file.

   f) Specify a label for the certificate. It can be any name.

   g) Click **Save**.

Chapter 4. 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.

All IBM Security Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See "Installing the dispatcher" on page 17.

Depending on your adapter, the Security Directory Integrator connector might already be installed as part of the Security Directory Integrator product and no further action is required. If the connector is not pre-installed, install it after the Dispatcher.

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*.

Related concepts

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

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 `PeopleSoftConnector.jar` file from the adapter package to the `ITDI_HOME/jars/connectors` directory.
4. Restart the adapter service.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

Installing 3rd party client libraries

Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

About this task

Procedure

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Setting up the adapter environment

In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

About this task

Procedure

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Loading the project

The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

About this task

The PeopleSoft HR feed adapter software contains component interfaces in the `ENROLE_PERSON` subdirectory of the `PT854_HRFEEDCOMPONENT.zip` file for PeopleTools 8.54.

This `ENROLE_PERSON` subdirectory is imported into the PeopleSoft Application Designer as a PeopleTools project.

Procedure

1. Copy the project into the PeopleTools system. See “Loading the component interfaces” on page 26.
2. Configure the project security. See “Setting the component interface security” on page 27.
3. Obtain and generate the PeopleSoft resource-specific JAR files. See “Resource-specific JAR files” on page 27.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Loading the component interfaces

You must import the ENROLE_PERSON directory into the PeopleSoft Application Designer as a PeopleTools project.

Procedure

1. Download the PT854_HRFEEDCOMPONENT.zip file if you haven't done so.
2. Extract PeopleTools and its contents into a temporary directory on your file system.
3. Log in to the PeopleSoft Application Designer in two-tier mode by using the PeopleTools account of the adapter.
   a) Select **Start** > **Programs** > **Peopletools8.5x** > **Configuration Manager**.
   b) Select the appropriate database type. For example, if PeopleSoft is configured with Oracle, select ORACLE.
   c) Specify the server name, database name, and other details for the database type, if not already specified.
   d) Click **OK**.
4. Copy the ENROLE_PERSON project.
   a) Log on to the PeopleSoft Application Designer.
   b) From the **Tools** menu, select **Copy Project** > **From File**.
   c) Browse to the directory where you extracted ENROLE_PERSON, which is displayed in the **Projects:** list area.
   d) Highlight ENROLE_PERSON and click **Select**.
      The ENROLE_PERSON project is loaded.
   e) Highlight the Component Interface and click **Copy**.
      The component interfaces are loaded into PeopleTools.
5. Exit the PeopleSoft Application Designer.

Related concepts
Resource-specific JAR files

The PeopleSoft HR feed adapter uses Java APIs to communicate and perform operations on the PeopleSoft resource.

Related tasks

Setting the component interface security
You must add components to the permissions list to set security for the PeopleTools project. It is necessary to secure the PeopleTools component interfaces.

Setting the component interface security

You must add components to the permissions list to set security for the PeopleTools project. It is necessary to secure the PeopleTools component interfaces.

About this task

Each individual method must also be secured. Security for the component interface is provided through the PeopleSoft Internet Architecture pages. Component interface permissions are set at the permission list level in PeopleSoft security

Procedure

1. Log in to the PeopleSoft web interface by using the PeopleTools account of the adapter.
2. From the PeopleSoft menu tree, select **PeopleTools** > **Security** > **Permissions & Roles** > **Permission Lists**.
3. Search for the **ALLPAGES** permission list link. The Permission List component is displayed.
4. Click **Component Interface** tab and add the following component interfaces to the list:

```
CI_PERSONAL_DATA
CI_JOB_DATA
```

5. Set Full Access for each method of the component interfaces that were added in the previous step.
6. Save your changes.

Related concepts

Resource-specific JAR files
The PeopleSoft HR feed adapter uses Java APIs to communicate and perform operations on the PeopleSoft resource.

Related tasks

Loading the component interfaces
You must import the ENROLE_PERSON directory into the PeopleSoft Application Designer as a PeopleTools project.

Resource-specific JAR files

The PeopleSoft HR feed adapter uses Java APIs to communicate and perform operations on the PeopleSoft resource.

The PeopleSoft HR feed adapter requires the following JAR files:

CompIntfc.jar
The Java API JAR file for the **ENROLE_PERSON** Component Interface project.

psjoa.jar
This JAR file is created during the PeopleTools installation. The path to the `psjoa.jar` file must be set to the *ITDI CLASSPATH* variable.

psft.jar
See "Creating a psft.jar file" on page 28.

JDBC type 4 driver JAR file
This JAR file is required to establish the connection with the database.

Related tasks

Loading the component interfaces
You must import the ENROLE_PERSON directory into the PeopleSoft Application Designer as a PeopleTools project.

Setting the component interface security
You must add components to the permissions list to set security for the PeopleTools project. It is necessary to secure the PeopleTools component interfaces.

Creating a psft.jar file

Procedure

1. Go to the workstation where PeopleTools is installed.
2. Locate the PSKeyStore.class file that is present in the pshttp folder of PeopleTools. It is in the web server installation directory. For example:

   Oracle WebLogic Service

   PS_HOME\webserv\web_server\applications\peoplesoft\PORTAL.war\ WEB-INF \classes\psft\pt8\pshttp

   IBM WebSphere

   PS_HOME\webserv\profile_name\installedApps\app_name\NodeCell\app_name.ear \PORTAL.war\ WEB-INF\classes\psft\pt8\pshttp
3. Copy the pshttp folder to a temporary folder that contains a psft\pt8 folder structure. For example, C:\Temp\psft\pt8\pshttp
4. Go to command prompt and locate the temporary folder that contains the psft/pt8/pshttp folder structure. For example, C:\Temp
5. From the command prompt, create the psft.jar file with the following command: jar -cvf psft.jar psft

   After the command is successfully completed, a psft.jar file is created on the temp folder.
6. On the workstation where IBM Security Directory Integrator is installed, copy the psft.jar file to the folder *ITDI_HOME*\jars\3rdParty\others.

Related concepts

psjoa.jar file
This file is created in the *PEOPLESOFT_HOME*\web\psjoa directory during the PeopleTools installation.

JDBC type 4 driver JAR file
By default, the **find** method of a PeopleSoft Component Interface is limited to a maximum of 300 entries from PeopleSoft. If your require more than 300 entries, the PeopleSoft Connector must invoke JDBC queries on the PeopleSoft database tables.

Related tasks

Generating the CompIntfc.jar file
You must create the CompIntfc.jar file from the Component interface JAVA files. The CompIntfc.jar file is the PeopleSoft Component Interface JAR file.

Generating the CompIntfc.jar file

You must create the CompIntfc.jar file from the Component interface JAVA files. The CompIntfc.jar file is the PeopleSoft Component Interface JAR file.

About this task

This file must be generated from the respective PeopleSoft resource and then copied to the *ITDI_HOME* \jars\3rdParty\others directory on the workstation where the adapter is installed.

Procedure

1. Log on to PeopleSoft Application Designer in two-tier mode.
2. Open the ENROLE_PERSON Component Interface project.
3. Open all the component interfaces by double-clicking each component interface.
4. From the menu, select **Build** > **PeopleSoft APIs**.
5. From the Build PeopleSoft API Bindings window, select the Java classes **Build** check box.
6. Clear the COM Type Library and C Header Files **Build** check boxes.
7. In the Java Classes frame, select the **Build** check box.
8. Select the appropriate Component Interfaces from the list and click **OK**.

   Note:

   - If you must generate Component Interface Java files for the entire group of Component Interfaces, click **ALL**.
   - Specify the file path for the Java files or let the files be generated in the default location, *PEOPLESOFT_HOME*\web\psjoa.

     The Component Interface Java files are put in a subdirectory called PeopleSoft\Generated\CompIntfc directory that is created in the specified location. For example, if you specified e:\enrole as the file path, then the Component Interface Java files are generated in the e:\enrole\PeopleSoft\Generated\CompIntfc directory.
   - When you generate the CompIntfc.jar, add the psjoa.jar file to the environment variable classpath. For example, if c:\PT8.54\class\psjoa.jar is the location, then add C:\PT8.54\class\ to the classpath environment variable.
9. Compile the Java files.
   a) Open the command prompt and go the directory where the generated Java files are located.

      For example,

      ```
      cd e:\enrole
      ```

   b) Go to the PeopleSoft\Generated\CompIntfc\ directory.
   c) Run the following command.

      ```
      javac -classpath <people tools install folder>\peoplesoftNodeCell
      \peoplesoft.ear\PORTAL.war\WEB-INF\classes *.java
      ```

      For example:

      ```
      javac -classpath C:\Users\Administrator\psft\pt\8.54\webserv\peoplesoft\
      installedApps\peoplesoftNodeCell\peoplesoft.ear\PORTAL.war\WEB-INF\
      classes *.java
      ```

   d) Optional: You can delete all the generated Java files except the .class files from the existing directory.
10. Package the compiled files as CompIntfc.jar file.
    a) Open the command prompt and go the directory where the generated Java files are located.

       For example,

       ```
       cd e:\enrole
       ```

    b) Run the following command:

       ```
       jar –cvf CompIntfc.jar *
       ```

    Note: Ensure that the Java compiler that is used for compiling the generated Java files is compatible with both

    - The Java provided with the PeopleSoft managed resource

- The Java provided with Security Directory Integrator

11. Copy the generated `CompIntfc.jar` file to the *ITDI_HOME*`\jars\3rdParty\others` directory.
12. For PeopleTools 8.54, copy the `com` folder from `\installedApps\peoplesoftNodeCell \peoplesoft.ear\PORTAL.war\WEB-INF\classes` to `ITDI_HOME\jars\3rdparty\others`.

Related concepts

psjoa.jar file
This file is created in the *PEOPLESOFT_HOME*`\web\psjoa` directory during the PeopleTools installation.

JDBC type 4 driver JAR file
By default, the **find** method of a PeopleSoft Component Interface is limited to a maximum of 300 entries from PeopleSoft. If your require more than 300 entries, the PeopleSoft Connector must invoke JDBC queries on the PeopleSoft database tables.

Related tasks

Creating a psft.jar file

psjoa.jar file

This file is created in the *PEOPLESOFT_HOME*`\web\psjoa` directory during the PeopleTools installation.

You must copy the `psjoa.jar` file from *PEOPLESOFT_HOME*`\web\psjoa` to the *ITDI_HOME*`\jars \3rdParty\others` directory on the workstation where the adapter is installed.

Related concepts

JDBC type 4 driver JAR file
By default, the **find** method of a PeopleSoft Component Interface is limited to a maximum of 300 entries from PeopleSoft. If your require more than 300 entries, the PeopleSoft Connector must invoke JDBC queries on the PeopleSoft database tables.

Related tasks

Creating a psft.jar file

Generating the CompIntfc.jar file
You must create the `CompIntfc.jar` file from the `Component interface` JAVA files. The `CompIntfc.jar` file is the PeopleSoft Component Interface JAR file.

JDBC type 4 driver JAR file

By default, the **find** method of a PeopleSoft Component Interface is limited to a maximum of 300 entries from PeopleSoft. If your require more than 300 entries, the PeopleSoft Connector must invoke JDBC queries on the PeopleSoft database tables.

Copy the *JDBC_driver*`.jar` that is used by PeopleSoft database to *ITDI_HOME*`\jars\3rdParty \others` directory.

The PeopleSoft HR feed adapter establishes the connection directly with the database if it finds more than 300 records to be retrieve. The PeopleSoft HR feed adapter uses the JDBC Type 4 drivers to retrieve more than 300 records. To establish the connection to the database, you must specify the appropriate driver class and a URL of the correct format.

For example:

PeopleSoft configured with the DB2®:

JDBC Drivers:
`db2jcc.jar db2jcc_javax.jar db2jcc_license_cu.jar`

Driver Class
`com.ibm.db2.jcc.DB2Driver`

URL
`jdbc:db2://`*`workstation`*`:50000/`*`database`*

PeopleSoft configured with the Microsoft SQL Server 2005:

JDBC Drivers:
`sqljdbc4.jar`

Driver Class
com.microsoft.sqlserver.jdbc.SQLServerDriver

URL
`jdbc:sqlserver://`*`workstation_name`*`:`*`port`*`;`
`instanceName=`*`instance`*`;SelectMethod=curson;DatabaseName=`*`database`*

What to do next

After you finish the adapter installation, do the following tasks:

- "Verifying the adapter installation" on page 31.
- Importing the adapter profile.
- Creating an adapter service.

  You must provide the account information when you create a service and ensure that the account has sufficient privileges to administer the PeopleSoft Application server users.

Related concepts

psjoa.jar file
This file is created in the *PEOPLESOFT_HOME*`\web\psjoa` directory during the PeopleTools installation.

Related tasks

Creating a psft.jar file

Generating the CompIntfc.jar file
You must create the `CompIntfc.jar` file from the `Component interface JAVA` files. The `CompIntfc.jar` file is the PeopleSoft Component Interface JAR file.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Windows operating system
`drive``:\Program Files\IBM\TDI\V7.2\jars\connectors\`

UNIX operating system
`/opt/IBM/TDI/V7.2/jars/connectors/`

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

Related concepts

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.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details

Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping

Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

About this task

The **USER_ADD** flow process does not include the **Generate Unique UserID** rule by default. You must manually add the **Generate Unique UserID** rule before you can successfully import HR feed data.

Procedure

1. Log in to the IBM Security Identity Governance and Intelligence Administration Console.
2. Click **Access Governance Core**.
3. Click **Configure** > **Rules** > **Rules**.
4. In the **Rules** tab on the left pane, complete the following fields:
   a) In the **Rule Class** field, select **Live Events**.
   b) In the **Queue** field, select **IN**.
   c) In the **Rule Flow** field, select **USER_ADD**.
5. In the **USER_ADD** flow process, expand and select the **User Add default group** folder for the rule group.
6. In the right pane, expand **Rules Package**.
7. In the **Rules Package** pane, select **Generate Unique UserID**.
8. From the **Actions** menu, click **Add**.
   In the left pane, **Generate Unique UserID** is displayed in the rule group that is named **User Add default group**.
9. In the left pane, move **Generate Unique UserID** so it is located after **Create OrgUnit From User Data** before **Create User**.
10. Restart the IBM Security Identity Governance and Intelligence server.
    a) On the **Appliance Dashboard** of the Security Identity Governance and Intelligence virtual appliance console, locate the **Server Control** widget.
    b) Select .
    c) Click **Restart**.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector

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

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Restarting the adapter service

Various installation and configuration tasks 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*.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Service/Target form details

Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping

Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Before you begin

- The IBM Security Identity server is installed and running.
- You have root or administrator authority on the IBM Security Identity 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 Identity Manager is located in the top level folder 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.

Procedure

1. Log on to the IBM Security Identity 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.
   For example, if you are installing the IBM Security Identity Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` 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 Identity 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. The `enRoleLogging.properties` file is in the IBM Security Identity server*HOME*`\data` directory. .

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Before you begin

- You have root or administrator authority on the IBM Security Identity 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 Identity Manager is located in the top level folder 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.

The adapter profile is already imported into the IBM Security Identity Manager virtual appliance. Read the adapter release notes for any specific instructions before you import a new adapter profile on IBM Security Identity Manager.

Procedure

1. Log on to the IBM Security Identity 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.
   For example, if you are installing the IBM Security Identity Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` 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 Identity 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. The `enRoleLogging.properties` file is in the IBM Security Identity server*HOME*`\data` directory. .

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR

file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Before you begin

- The IBM Security Privileged Identity Manager is installed and running.
- You have root or administrator authority on the IBM Security Privileged Identity Manager.
- 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 Privileged Identity Manager is located in the top level folder 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.

Procedure

1. Log on to the IBM Security Privileged Identity Manager 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.
For example, if you are installing the IBM Security Identity Adapter for a Windows server that runs Active Directory, locate and import the ADProfileJAR 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 Identity 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. The enRoleLogging.properties file is in the IBM Security Identity server*HOME*\data directory. .

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

Importing the adapter profile

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

Before you begin

- The IBM Security Identity Governance and Intelligence server is installed and running.
- You have administrator authority on the IBM Security Identity Governance and Intelligence 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.

About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Identity Adapter. The adapter profile must be imported because it defines the types of resources that the Security Identity Governance and Intelligence server can manage.

The adapter profile definition file is used to create a target profile on the Security Identity Governance and Intelligence server and to establish communication with the adapter. If the adapter profile is not imported, you cannot create a connector for that adapter type.

An upload error might occur when no file is selected, or when the file is empty, or due to any upload operation error, such as a timeout or connection error. If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a connector with the adapter profile or open and account on the service. You must import the adapter profile again.

This task can be completed from the Enterprise Connectors module in the Administration Console. To import an adapter target profile, complete these steps:

Procedure

1. Log in to the Security Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Profile**.
   b) Click **Browse** to locate the JAR file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported a profile.
7. Click **Close**.
   The new profile is displayed in the list of profiles.

Results

The upload is synchronous but has a timeout. The progress bar on the **Import** page accurately indicates the upload status. However, when a timeout is reached, the following message occurs: "The import is still

in progress and will complete shortly. Close this window to proceed." If you see that message, allow a few minutes for the upload to complete and for the profile to be available.

What to do next

After the target profile is imported successfully, complete these tasks.

- Import the attribute mapping file. See "Importing attribute mapping file" on page 47.
- Create a connector that uses the target profile. See "Adding a connector" on page 49.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Importing attribute mapping file

After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

About this task

This task involves importing an account attribute mapping definition file, which is included in the adapter package. The imported file must be a DEF file.

Procedure

1. Log in to the Security Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Profiles**.

4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions** > **Import**.
6. On the **Import** page, complete these steps:
   a) Select **Attribute Mapping**.
   b) Click **Browse** to locate the attribute mapping file that you want to import.
   c) Click **Upload file**.
   A message indicates that you successfully imported the file.
7. Click **Close**.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Adding a connector

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

Before you begin

Complete Importing the adapter profile.

Note: If you migrated from Security Identity Governance and Intelligence V5.2.2 or V5.2.2.1 and want to add or configure a connector, see *Adding and configuring a connector for each target* in the IBM Security Identity Governance and Intelligence product documentation.

About this task

The connectors consolidate, extract, and reconcile user identities, organization units, permissions, and user entitlements with the most common enterprise applications. Configure a connector to keep the Access Governance Core repository synchronized with the target system.

This task can be completed from the Enterprise Connectors module in the Administration Console.

Procedure

To add a connector, complete these steps.

1. Log in to the Security Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.
   The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
   a) Assign a name and description for the connector.
   b) Select the target profile type as `Identity Brokerage` and its corresponding target profile.
   c) Select the entity, such as **Account** or **User**.
      Depending on the connector type, this field might be preselected.
   d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
      The available trace levels are DEBUG, INFO, and ERROR.
   e) Optional: Select **History ON** to save and track the connector usage.
   f) Click **Save**.
      The fields for enabling the channels for sending and receiving data are now visible.
   g) Select and set the connector properties in the **Global Config** accordion pane.
      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

The connector is saved and added to the list of connectors in the **Connectors** pane.

If you cannot create a connector with the target profile or open an account on an existing connector, the target profile was not installed correctly during the import. You must import the target profile again.

What to do next

Enable the channel modes to synchronize the data between the target systems and Security Identity Governance and Intelligence. For more information, see “Enabling connectors” on page 52.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Before you begin

Table 6. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Security Identity Governance and Intelligence.	"Adding a connector" on page 49.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 55.

Procedure

To enable a connector, complete these steps:

1. Log in to the Security Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.
   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

Enable write-to channel
Propagates every change in the Access Governance Core repository into the target system.

For connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

Enable read-from channel
Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

For HR feed connectors, only the check box for enabling the read-from channel is available.

Enable reconciliation
Synchronizes the modified data between the Access Governance Core repository and the target system.

Results
The connector is enabled

What to do next

Enable the channel modes to synchronize the data between the target systems and Security Identity Governance and Intelligence.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

About this task

Note: Legacy Security Identity Governance and Intelligence Enterprise connectors use `Reconciliation` channel, whereas Identity Brokerage Enterprise connectors use `Read From Channel` and `Change Log Sync`.

For more information about any of tasks in the following steps, see the IBM® Security Identity Governance and Intelligence product documentation.

Procedure

To enable the read-from and write-to channels, and to set the change log synchronization schedule for each new connector, complete these steps in Security Identity Governance and Intelligence V5.2.3:

1. Log in to the Security Identity Governance and Intelligence Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

      Enable write-to channel
      Propagates every change in the Access Governance Core repository into the target system.

      Enable read-from channel
      Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.

      Enable reconciliation
      Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
   b) Select a connector, and click **Actions** > **Sync Now**.

      The synchronization process begins.
   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.

      Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.

11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.
    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    c) Click **Save**.

    For more information, see "Enabling connectors" on page 52.

    For Identity Brokerage connectors that are not HR feed, the check boxes for enabling the read-from channel and the write-to channel are available.

    For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.
12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

About this task

This task involves either an user or OU attribute mapping definition file, which are both included in the HR adapter package.

The file consists of Security Identity Governance and Intelligence user or OU attributes and their equivalent attributes in the managed HR target. The file is structured as *<IGI_attribute> = <HR_target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<HR_target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<HR_target_attribute>* of `ersaphraccounterptigiuseraccount`. For example:

```
GIVEN_NAME=ersaphrgivennameerptigifirstName
```

Some *<IGI_attribute>* do not have a defined *<HR_target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Security Identity Governance and Intelligence attribute values.

   ```
   [conversion].<HR_target_attribute>.<IGI_attribute> =
   [<HR_target_attribute_value1>=<IGI_attribute_value1>;...;
   <HR_target_attribute_valuen>=<IGI_attribute_valuen>]
   ```

   For example:

   ```
   [conversion].ersaphrgender.GENDER=[M=0;F=1;U=]
   ```

   ```
   [conversion].erptigidisabled.DISABLED=[Y=1;N=0]
   [conversion].erptigigender.GENDER=[M=0;F=1]
   ```

4. For attributes that contains date and time, use the following syntax to convert its values.
   For example:

   ```
   [conversion.date].ersaphrdoberptigibirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]
   [conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=
   [dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]
   ```

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Identity Governance and Intelligence product documentation.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector

Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Attribute mapping

Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

About this task

This task involves either an user or OU attribute mapping definition file, which are both included in the HR adapter package.

The file consists of Security Identity Governance and Intelligence user or OU attributes and their equivalent attributes in the managed HR target. The file is structured as *<IGI_attribute> = <HR_target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<HR_target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<HR_target_attribute>* of `ersaphraccounterptigiuseraccount`. For example:

```
GIVEN_NAME=ersaphrgivennameerptigifirstName
```

Some *<IGI_attribute>* do not have a defined *<HR_target_attribute>* and you can assign the mapping. For example:

```
USER_TYPE=USER_TYPE
ATTR1=ATTR1
```

Note:

- The default mapping is already included out-of-the box. If there are no changes to the attribute mapping, there is no need to import the attribute mapping files.
- It might take up to 10 minutes for the attribute mapping changes to take effect once the file is imported.

Procedure

1. Open the mapping definition file by using any text editor.
2. Edit the mapping.
3. If the target attribute has a list of predefined values, use the following syntax to convert its values to the corresponding Security Identity Governance and Intelligence attribute values.

```
[conversion].<HR_target_attribute>.<IGI_attribute> =
[<HR_target_attribute_value1>=<IGI_attribute_value1>;...;
<HR_target_attribute_valuen>=<IGI_attribute_valuen>]
```

For example:

```
[conversion].ersaphrgender.GENDER=[M=0;F=1;U=]
```

```
[conversion].erptigidisabled.DISABLED=[Y=1;N=0]
[conversion].erptigigender.GENDER=[M=0;F=1]
```

4. For attributes that contains date and time, use the following syntax to convert its values.
   For example:

```
[conversion.date].ersaphrdoberptigibirthDate.BIRTHDAY=[yyyyMMdd=dd/MM/yyyy HH:mm:ss]
[conversion.date].ACCOUNT_EXPIRY_DATE.ACCOUNT_EXPIRY_DATE=
[dd/MM/yyyy HH:mm:ss=dd/MM/yyyy HH:mm:ss]
```

5. Import the updated mapping definition file through the Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Identity Governance and Intelligence product documentation.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

“Adapter attributes” on page 93
The IBM Security Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project

The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

Creating an adapter service/target

After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Before you begin

Complete "Importing the adapter profile" on page 37.

About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form 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

1. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. 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:
      - Click the arrow to go to the next page.
      - 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**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. 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:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

```
<Domain Name>\<Login Name>
```

8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

    Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

    The adapter must be running to obtain the information.
12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

    The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.
13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

    The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.
14. Optional: On the **Service Information** or **General Information** page, 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 analyst who is responsible for the computer on which the managed resource runs.

Results

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

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details

Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping

Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Creating an adapter service/target

After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Before you begin

Complete “Importing the adapter profile” on page 39.

About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form 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

1. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. 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:
      - Click the arrow to go to the next page.
      - 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**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.

5. 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:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.

   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

   ```
   <Domain Name>\<Login Name>
   ```
8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

    Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

    The adapter must be running to obtain the information.
12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

    The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.
13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

    The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.
14. Optional: On the **Service Information** or **General Information** page, 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 analyst who is responsible for the computer on which the managed resource runs.

Results

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

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors

After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Creating an adapter service/target

After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Before you begin

Complete “Importing the adapter profile” on page 42.

About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form 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

1. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Services** table, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. 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:

- Click the arrow to go to the next page.
- 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**.

The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.

5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
6. On the **Service Information** page, specify the appropriate values for the service instance.

   The content of the **Service Information** page depends on the type of service that you are creating.
7. Click **Test Connection** to validate that the data in the fields is correct.

   If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.
8. Click **Finish**.

Results

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

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project

The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

Service/Target form details

Complete the service/target form fields.

The PeopleSoft HR feed adapter service form has several tabs, each containing information that you must specify:

- “General Information tab” on page 74
- “Connection Details tab” on page 74
- “Dispatcher Attributes tab” on page 75

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.

- JDBC driver
- JDBC URL
- Database user name
- Database user password
- Assembly Line File System path
- Max connection count

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID

Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Verifying that the adapter is working correctly

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

General Information tab

This tab provides general information about the adapter service.

Service Name
Specify a name that defines the adapter service on the IBM Security Identity Governance and Intelligence server.

Note: Do not use forward (/) or backward slashes (\) in the service name.

Description
Optional: Specify a description that identifies the service for your environment.

IBM Security Directory Integrator location

Optional: 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. `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*.

Connection Details tab

This tab describes the parameters that have to be specified to establish a remote connection to the PeopleSoft resource from IBM Security Directory Integrator.

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.

- JDBC driver
- JDBC URL
- Database user name
- Database user password

APP Server name
Specify the name or IP address of the PeopleTools Application Server to be managed.

APP Server port
Specify the port number that connects to the PeopleTools Application Server. It is the IP port number on which the PeopleTools Application Server listens for JOLT connections. The value is typically port 9000.

PS APP ID
Specify the name of the PeopleTools account that is created for the adapter.

APP ID password
Specify a password of the PeopleTools account that is created for the adapter.

JDBC driver
Specify the database type 4 JDBC driver. For example, the JDBC driver for IBM DB2 database connectivity is `com.ibm.db2.jcc.DB2Driver`.

JDBC URL
Specify the web address that connects to the PeopleSoft tables. For example, the connectivity JDBC URL for IBM DB2 database is `jdbc:db2://10.77.68.37:50000/PTDB jdbc:db2://ip address:port/database name`.

Database user name
Specify the administrator user name that connects to the database.

Database user password
Specify the password for the database user.

PeopleTools Domain Password
The domain connection password. Specify the password for the PeopleTools domain if it is configured. The password is optional on the PeopleSoft resource.

Database table owner
Specify the name of the PeopleTools database table owner.

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.

- Assembly Line File System path
- Max connection count

Assembly Line File System 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 Identity Governance and Intelligence.

For example:

Windows operating system
```
C:\Program Files\IBM\TDI\V7.2\profiles
```

UNIX and Linux® operating system
```
/opt/IBM/TDI/V7.2/profiles
```

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.

Select 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 PeopleSoft resource is maintained. The next request that the adapter receives can reuse this connection.

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

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.

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 Identity serverIBM Security Identity Governance and Intelligence server.

2. Run a full reconciliation from the IBM Security Identity serverIBM Security Identity Governance and Intelligence server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector
After you import the adapter profile on the Security Identity Governance and Intelligence server, add a connector so that Security Identity Governance and Intelligence server can communicate with the managed resource.

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

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 Identity Governance and Intelligence server.
2. Run a full reconciliation from the IBM Security Identity Governance and Intelligence server.
3. Run all supported operations such as add, modify, and delete on one user account.
4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts
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.

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 JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service
Various installation and configuration tasks 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.

Service/Target form details
Complete the service/target form fields.

Related tasks

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.

Installing 3rd party client libraries
Third party client libraries are libraries and/or configuration files that are provided by the target vendor. These 3rd party client libraries must be installed with the adapter. This is not required for all adapters.This topic is not applicable for this adapter.

Setting up the adapter environment
In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

Loading the project
The adapter package includes a compressed file that contains the PeopleTools project file. The project file has component interfaces that must be imported into the PeopleSoft Application Designer.

Configuring the rule for the unique user ID
Complete this task to configure the rule for the unique user ID for HR feed profiles. You must add the **Generate Unique UserID** rule to the **USER_ADD** flow process.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Importing the adapter profile
You can import a profile definition file, which creates a profile in IBM Security Identity Governance and Intelligence server. Use this option for importing adapter profiles.

Importing attribute mapping file
After importing the adapter profile, you must import an attribute map from a profile mapping definition file.

Adding a connector

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

Enabling connectors
After you create a connector, by default it is in a disabled state. You must enable a connector to use it.

Reviewing and setting channel modes for each new connector
Use this procedure to set up the read-from and write-to channels and to set the synchronization schedule for each new connector.

Attribute Mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Attribute mapping
Attribute mapping is required to define which target attributes correspond to the Security Identity Governance and Intelligence user or OU attributes.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Creating an adapter service/target
After you import the adapter profile on the IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Chapter 5. Upgrading

Upgrading an IBM Security Directory Integrator-based adapter involves tasks such as upgrading the dispatcher, the connector, and the adapter profile. Depending on the adapter, some of these tasks might not be applicable. Other tasks might also be required to complete the upgrade.

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

Upgrading the Dispatcher

The new adapter package might require an upgrade of 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.

Related concepts

Upgrading the adapter profile

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

Upgrading the adapter profile

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.

Related concepts

Upgrading the Dispatcher

The new adapter package might require an upgrade of the Dispatcher.

Chapter 6. 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

Customizing the adapter profile

You can customize the adapter profile to change the account form or the service form. To customize the adapter profile, you must modify the adapter JAR file.

About this task

Use the Form Designer or the `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file.

The JAR file is included in the adapter package that you downloaded from the IBM Passport Advantage website. The JAR file and the files in the JAR file vary depending on your operating system.

The `adapter` JAR file includes the following files:

- `CustomLabels.properties`
- `erptigirmiservice.xml`
- `erptigiuseraccount.xml`
- `IGIPeopleToolsSearchAL.xml`
- `IGIPeopleToolsTestAL.xml`
- `schema.dsml`
- `service.def`

Procedure

1. Edit the JAR file.
   a) Log on to the workstation where the PeopleSoft HR feed adapter is installed.
   b) On the **Start** menu, select **Programs → Accessories → Command Prompt**.
   c) Copy the JAR file into a temporary directory.
   d) Extract the contents of the JAR file into the temporary directory by running the following command. Type the name of the JAR file for your operating system.
   The following example applies to the PeopleSoft HR feed adapter profile.

   ```
   cd c:\temp cd /tmp
   jar -xvf PeopleSoftHRProfile.jar
   ```

   The **`jar`** command extracts the files into the `PeopleSoftHRProfile` directory.
   e) Edit the file that you want to change.

After you edit the file, you must import the file into the IBM Security Identity server for the changes to take effect.

2. Import the file.
   a) Create a JAR file by using the files in the directory.

      Run the following commands:

      Windows

      ```
      cd c:\temp
      jar -cvf PeopleSoftHRProfile.jar PeopleSoftHRProfile
      ```

      UNIX

      ```
      cd /tmp
      jar -cvf PeopleSoftHRProfile.jar PeopleSoftHRProfile
      ```

   b) Import the JAR file into the IBM Security Identity ManagerIBM Security Identity Governance and IntelligenceIBM Security Privileged Identity Manager application server.

   c) Stop and start the IBM Security Identity server

   d) Restart the adapter service.

Related concepts

Preparing an MS-DOS ASCII file on the UNIX or Linux operating system

The adapter profile `.jar` file might contain ASCII files in MS-DOS ASCII format.

Preparing an MS-DOS ASCII file on the UNIX or Linux operating system

The adapter profile `.jar` file might contain ASCII files in MS-DOS ASCII format.

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a `^M` character at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with running the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the `^M` characters.

You can use the **vi** editor to remove the `^M` characters manually. From the **vi** command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter `^M` or `Ctrl-M` by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as a command.

Related tasks

Customizing the adapter profile

You can customize the adapter profile to change the account form or the service form. To customize the adapter profile, you must modify the adapter JAR file.

Chapter 7. 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?

Related concepts

Configuring debugging
By default, adapters log message in "INFO" level. In order to force the adapter to log detailed message, you must enable "DEBUG" level logging.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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.

Configuring debugging

By default, adapters log message in "INFO" level. In order to force the adapter to log detailed message, you must enable "DEBUG" level logging.

Related concepts

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.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

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.

Logs

When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

```
<Log Level> [<Assembly Line_ProfileName>_<Request Id>]_
[<Connector Name>] - <message>
```

Log Level
Specifies the logging level that you configured for the adapter. The options are DEBUG, ERROR, INFO, and WARN. For information about using the `log4j.properties` file to configure logging, see the *Dispatcher Installation and Configuration Guide*.

Assembly Line
Specifies the name of the assembly line that is logging the information.

ProfileName
Specifies the name of the profile. Profile names can vary based on the adapter that is running or the operating system.

Request ID
Specifies the number of the request. The Request ID is used to uniquely identify a specific request.

Connector Name
Specifies the adapter connector.

Message
Specifies the informational message.

When you click the **Test** button on the service form, the service, environment, and configuration values are sent to the IBM Security Directory Integrator log during the test. These collected information can help diagnose issues.

The log files are kept in the UNIX System Services file system, under the installation path of the adapter, in the read/write `log` subdirectory.

The adapter log name is the adapter instance name, followed by an extension of `.log`. When the extension is `.log`, it is the current log file. Old log files have a different extension such as `.log_001`,`.log_002`, `.log_003` and so on.

Table 7. Example of Adapter log details	
Details	**Example values**
Installation path	`/usr/itim`
Adapter log name	
Log location	`/usr/itim/log/`
Log files	• `.log` • `.log_001` • `.log_002` • `.log_003`

You can use the UNIX System Services **obrowse** command **tail**, or any other UNIX based utility to inspect the adapter logs.

The size of a log file, the number of log files, the directory path, and the detailed level of logging are configured with the **agentCfg** program.

Related concepts

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.

Configuring debugging
By default, adapters log message in "INFO" level. In order to force the adapter to log detailed message, you must enable "DEBUG" level logging.

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.

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 8 on page 88 and Table 9 on page 89 contain warnings or errors, which might be displayed when the PeopleSoft HR feed adapter is installed on your system.

Table 8. 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.

Table 8. Specific messages and actions (continued)		
Message number	**Message**	**Action**
CTGIMT001E	The following error occurred. Error: Unable to connect to PeopleSoft Application server.	• Verify that the PeopleSoft Application Server is running. • Verify that the credentials that are specified on the service form of the PeopleSoft Application Server are correct. • Verify that the PeopleSoft administrator user name and password that is specified on the service form of the PeopleSoft Application Server are correct.

Table 9. General messages and actions	
Message	**Action**

`LoadConnectors:`
`java.lang.NoClassDefFoundError:`
`psft/pt8/joa/JOAException`
	The `psjoa.jar` file is missing. Verify that the file exists in the *ITDI_HOME*`/jars/3rdParty/IBM` directory.

`InitConnectors:`
`java.lang.Exception:`
`Unable to GetComponent Interface ABC_XYZ`
	The PeopleSoft Component Interface classes are not available. Complete the following steps:
	• Verify that the `CompIntfc.jar` file (which contains the ENROLE_PERSON Component Interface project classes) is in the jars subdirectory of the *ITDI_HOME* directory.
	• Verify that the `CompIntfc.jar` file contains classes for the required ENROLE_PERSON Component Interface project.
	• If necessary, add the path of the jars subdirectory to the *ITDI CLASSPATH* variable.

`The search failed due to a system error.`	Ensure that: • The `CompIntfc.jar` and `psjoa.jar` are in the appropriate locations of the Security Directory Integrator. • The ENROLE_PERSON Component Interface project is deployed on the PeopleSoft resource. • The network connection is not slow between the IBM Security Identity ManagerIBM Security Identity Governance and IntelligenceIBM Security Privileged Identity Manager and the Security Directory Integrator or the Security Directory Integrator and the managed resource.
`The application could not establish a connection to hostname.`	Ensure that SSH is enabled on the managed resource.

Table 9. General messages and actions (continued)	
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 Identity ManagerIBM Security Identity Governance and IntelligenceIBM Security Privileged Identity Manager to refresh the list of attribute names.

Related concepts

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.

Configuring debugging
By default, adapters log message in "INFO" level. In order to force the adapter to log detailed message, you must enable "DEBUG" level logging.

Logs
When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

Chapter 8. Uninstalling

To remove an adapter from the IBM Security Identity server for any reason, you must remove all the components that were added during installation. Uninstalling an IBM Security Directory Integrator-based adapter mainly involves removing the connector file and the adapter profile from the IBM Security Identity 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 Identity server. Before you delete the adapter profile, ensure that no objects exist on the IBM Security Identity server that reference the adapter profile.

Objects on the IBM Security Identity server that can reference the adapter profile:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

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 Identity ManagerIBM Security Identity Governance and IntelligenceIBM Security Privileged Identity Manager product documentation.

Chapter 9. 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

Adapter attributes and object classes are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter. The IBM Security Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.This topic is not applicable for this adapter.

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.This topic is not applicable for this adapter.

Special attributes

Certain attributes have special syntax and meaning that customers needs to be aware off. This information will be used to help the customer in how to supply the attribute value.This topic is not applicable for this adapter.

Adapter attributes

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

The PeopleSoft HR feed adapter supports a standard set of attributes for user information.

The mandatory attributes to create an account are:

- Person ID
- First Name
- Last Name

Table 10. Supported attributes

PeopleSoft HR feed adapter attribute name	Description	Required	Managed Resource Attribute
erUiD	Person ID	YES	EMPLID
erptigifirstName	First Name	YES	FIRST_NAME
erptigilastName	Last Name	YES	LAST_NAME
erptigigender	Gender	NO	SEX
erptigibirthDate	Birth date	NO	BIRTHDATE
erptigibirthPlace	Birth place	NO	BIRTHPLACE
erptigibirthCountry	Birth country	NO	BIRTHCOUNTRY

Table 10. Supported attributes (continued)			
PeopleSoft HR feed adapter attribute name	**Description**	**Required**	**Managed Resource Attribute**
erptigiaddress	Address	NO	ADDRESS1
erptigicity	City	NO	CITY
erptigicountry	Country	NO	COUNTRY
erptigizipcode	Zip Code	NO	POSTAL
erptigiphoneNumber	Phone No.	NO	PHONE
erptigiemail	Email address	NO	EMAIL
erptigidisabled	Disabled	NO	DISABLED
erptigiOU	Organization unit	NO	BUSINESS_UNIT
erEmpl_rcd	Employee record number	NO	EMPL_RCD
erptigiactionCause	Action cause	NO	ACTION
erptigiactionType	Action type	NO	ACTION_TYPE

USER_ERC attribute mapping

The following table lists which adapter attributes are mapped to the attributes stored in the IBM Security Identity ManagerIBM Security Identity Governance and IntelligenceIBM Security Privileged Identity Manager USER_ERC table.

Table 11. USER_ERC attribute mapping			
USER_ERC attributes	**Description**	**Required**	**PeopleSoft HR feed adapter attribute name**
ID	Table unique identifier. The sequence `user_erc_seq` might be called to generate this unique number.	YES	
PM_CODE	USER ID or User Code. It is not required. USER ID can be generated using a rule.	NO	
OU	Organizational unit code. Used to store the user in the OU available in the system. This attribute might or might not be in the database. Create the new OU in the `root`.	YES	**erptigiOU** Represents the OU assigned to the Person.

Table 11. USER_ERC attribute mapping (continued)

USER_ERC attributes	Description	Required	PeopleSoft HR feed adapter attribute name
USER_TYPE	User type name. This attribute might or might not be in the database. It can be created dynamically using a custom rule.	NO	
PROCESSED	Deprecated	NO	
LAST_MOD_USER	Contains the name of the last user or process that modified the USER_ERC table.	NO	
LAST_MOD_TIME	Contains the date and time when the last change occurred. Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed.	NO	
POST_EVENT	Deprecated	NO	
SKIP	Deprecated	NO	
ACTION_TYPE	SAP HR property information.	NO	**erptigiactionType**
ACTION_CAUSE	SAP HR property information.	NO	**erptigiactionCause**
ACTION_TYPE_LAST	SAP HR property information.	NO	
ACTION_CAUSE_LAST	SAP HR property information.	NO	
GIVEN_NAME	User name	YES	**erptigifirstName**
SURNAME	User surname	YES	**erptigilastName**
GENDER	• 0 = male • 1 = female	NO	**erptigigender**
BIRTHDAY	Birthday	NO	**erptigibirthDate**
BIRTH_PLACE	Birth place	NO	**erptigibirthPlace**
BIRTH_COUNTRY	Birth country	NO	**erptigibirthCountry**

Table 11. USER_ERC attribute mapping (continued)

USER_ERC attributes	Description	Required	PeopleSoft HR feed adapter attribute name
ACCOUNT_EXPIRY_DATE	The Security Identity Governance and Intelligence account can be created with an expiration date. Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed.	NO	
IDENTIFICATION_NUMBER	User ID present into HR system	NO	**erUid**
CURRENTOU	Deprecated	NO	
NATION	Nation	NO	
ZIPCODE	Zip code	NO	**erptigizipcode**
COUNTRY	Country	NO	**erptigicountry**
PHONE_NUMBER	Phone number	NO	**erptigiphoneNumber**
DISABLED	Indicates that the user is disabled and it disables all user accounts	NO	**erptigidisabled**
DELETED	Use this attribute to implement a particular logic when a user is deleted from HR system. For example, a user can keep all his account for 3 weeks and then the user is deleted	NO	
ATTR1	Spare attribute	NO	**erEmpl_rcd** Employee Record no. - EMPL_RCD is used for Multiple Jobs. Normally the 0 record is the Primary Job. This attribute is part of the OU information.
ATTR2	Spare attribute	NO	
ATTR3	Spare attribute	NO	
ATTR4	Spare attribute	NO	
ATTR5	Spare attribute	NO	
ATTR6	Spare attribute	NO	
ATTR7	Spare attribute	NO	
ATTR8	Spare attribute	NO	
ATTR9	Spare attribute	NO	

Table 11. USER_ERC attribute mapping (continued)			
USER_ERC attributes	**Description**	**Required**	**PeopleSoft HR feed adapter attribute name**
ATTR10	Spare attribute	NO	
ATTR11	Spare attribute	NO	
ATTR12	Spare attribute	NO	
ATTR13	Spare attribute	NO	
ATTR14	Spare attribute	NO	
ATTR15	Spare attribute	NO	
SCHEDULE	Deprecated	NO	
ADDRESS	User address	NO	**erptigiaddress**
CITY	User city	NO	**erptigicity**
EMAIL	User email	NO	**erptigiemail**

OrganizationalUnit_ERC attribute mapping

The following table lists which adapter attributes are mapped to the attributes stored in the IBM Security Identity ManagerIBM Security Identity Governance and IntelligenceIBM Security Privileged Identity Manager OrganizationalUnit_ERC table.

Table 12. OrganizationalUnit_ERC attribute mapping			
OrganizationalUnit_ERC attributes	**Description**	**Required**	**PeopleSoft HR feed adapter attribute name**
ID	Table unique identifier. The sequence `organizational_unit_erc_seq` might be called to generate this unique number.	YES	
PARENT	Organizational unit parent code This attribute might or might not be in the database. Create the new OU in the `root`.	NO	
OU	Organizational unit code (unique identifier)	YES	**erptigiOUName**
DESCRIPTION	Description	NO	**erptigidescr**
NAME	Organizational unit name	NO	**erptigidescrshort**
LAST_MOD_USER	Contains the name of the last user or process that modified the USER_ERC table.	NO	

Table 12. OrganizationalUnit_ERC attribute mapping (continued)

OrganizationalUnit_ERC attributes	Description	Required	PeopleSoft HR feed adapter attribute name
LAST_MOD_TIME	Contains the date and time when the last change occurred. Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed.	NO	
TIPO	Organizational unit type name. This attribute might or might not be in the database. It can be created dynamically using a custom rule.	NO	
SCHEDULE	Deprecated	NO	
ATTR1	Spare attribute	NO	**erptigidefaultsetid** Default `set_id` for OU support data.
ATTR2	Spare attribute	NO	
ATTR3	Spare attribute	NO	
ATTR4	Spare attribute	NO	
ATTR5	Spare attribute	NO	
ATTR6	Spare attribute	NO	
ATTR7	Spare attribute	NO	
ATTR8	Spare attribute	NO	
ATTR9	Spare attribute	NO	
ATTR10	Spare attribute	NO	
ATTR11	Spare attribute	NO	
ATTR12	Spare attribute	NO	
ATTR13	Spare attribute	NO	
ATTR14	Spare attribute	NO	
ATTR15	Spare attribute	NO	

Attributes by adapter actions

Each adapter action has required attributes. The adapter actions are grouped by function.

Test

To test the connection, use the attributes that are specified in the reference table.

Table 13. Test attributes	
Required attribute	**Optional attribute**
None	None

Related concepts

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Identity Governance and Intelligence and the adapter. To reconcile accounts, use the attributes that are specified in the reference table.

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Identity Governance and Intelligence and the adapter. To reconcile accounts, use the attributes that are specified in the reference table.

Table 14. Reconciliation request attributes	
Required attribute	**Optional attribute**
None	All other supported attributes

Related concepts

Test

To test the connection, use the attributes that are specified in the reference table.

Index

R

S

T

U

V

W