IBM Security Verify Governance Identity Manager

PeopleTools Adapter Installation and Configuration Guide

IBM

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The PeopleTools Adapter enables communication between the Identity server and the PeopleSoft server.

Adapters can be installed on the managed resource. The Identity server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

Features of the adapter

The adapter automates several administrative and management tasks.

The adapter automates the following tasks:

- Reconciling user accounts and support data, such as languages, currency code, roles, and permission lists.
- Adding, modifying, and deleting user accounts
- Modifying user account attributes
- Modifying user account password
- Checking the connection between the PeopleSoft Application Server and IBM® Security Verify Governance Identity Manager

Architecture of the adapter

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:

- The Dispatcher
- The IBM Security Directory Integrator connector
- IBM Security Verify Adapter profile

You must install the Dispatcher and the adapter profile; however, the Security Directory Integrator connector might already be installed with the base Security Directory Integrator product.

Figure 1 on page 2 describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

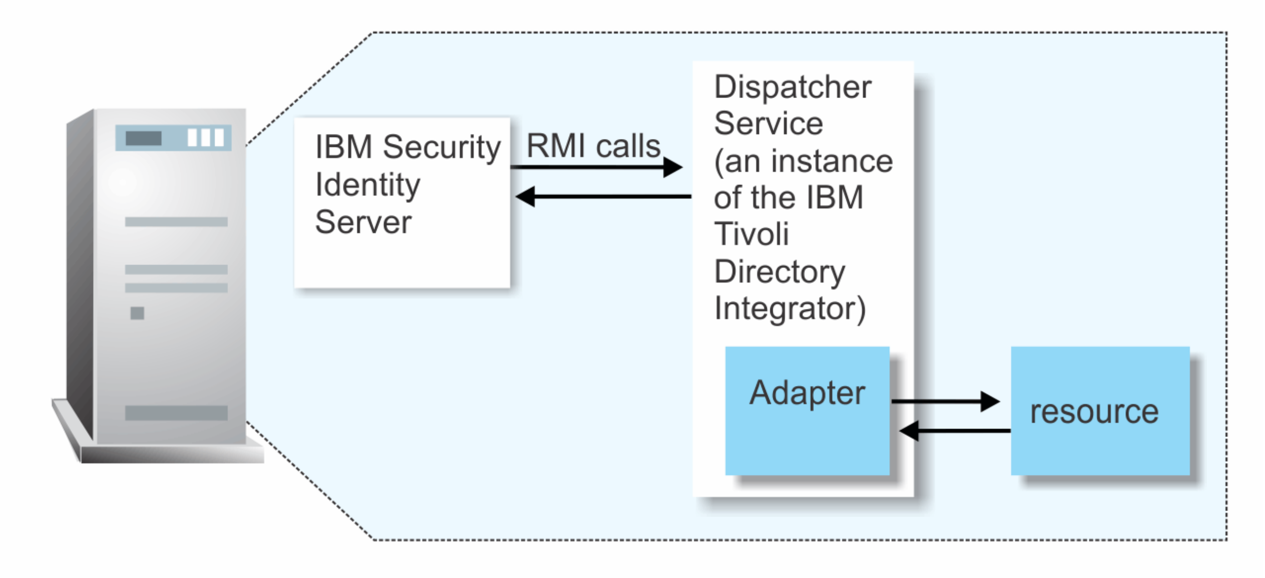
IBM Security Identity Server
RMI calls
Dispatcher Service (an instance of the IBM Tivoli Directory Integrator)
Adapter
resource

Figure 1. The architecture of the PeopleTools Adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

- The Identity server
- The IBM Security Directory Integrator server
- The managed resource
- The adapter

The adapter must reside directly on the server running the Security Directory Integrator server.

Single server configuration

In a single server configuration, install the Identity server, the Security Directory Integrator server, and the PeopleTools Adapter on one server to establish communication with the PeopleSoft Application Server.

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

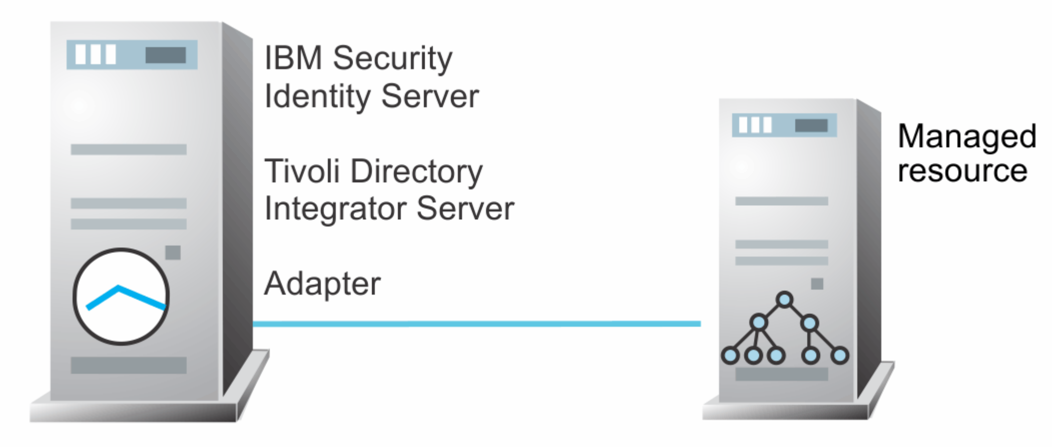
IBM Security Identity Server
Tivoli Directory Integrator Server
Adapter
Managed resource

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Identity server, the Security Directory Integrator server, the PeopleTools Adapter, and the PeopleSoft Application Server are installed on different servers.

Install theSecurity Directory Integrator server and the PeopleTools Adapter on the same server as described in Figure 3 on page 3.

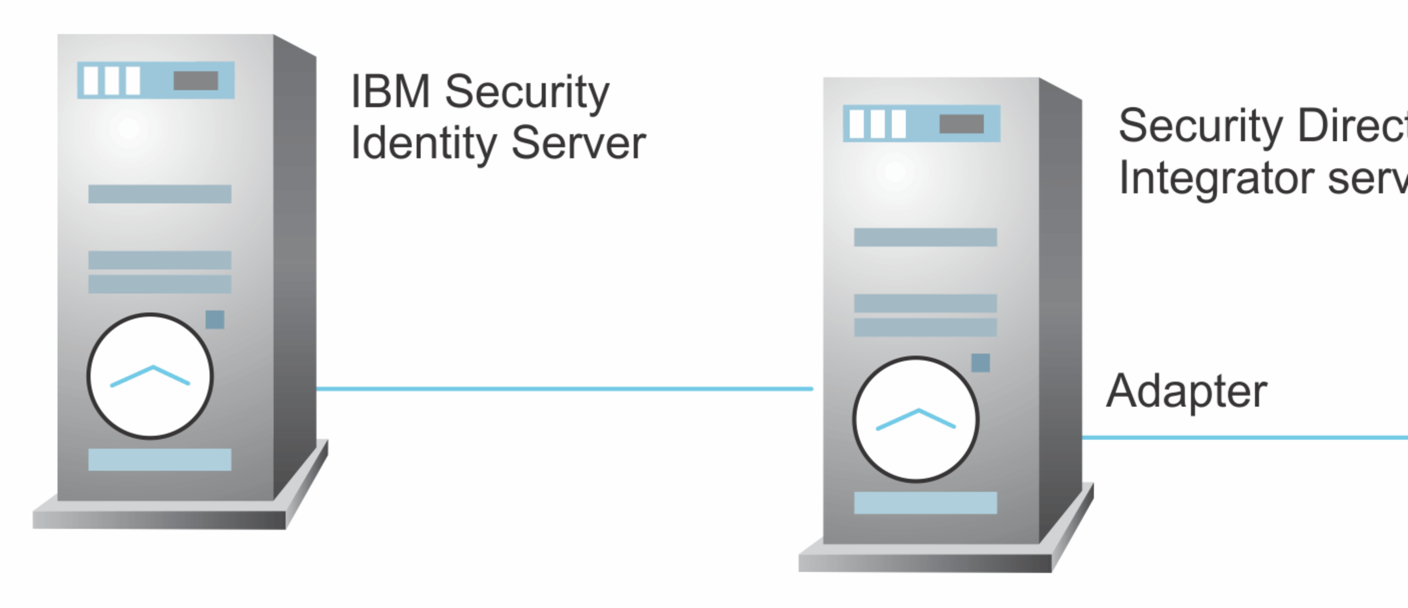

Figure 3. Example of a multiple server configuration

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.

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager

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 Verify Governance Identity Manager 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 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

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

Software downloads
Download the software through your account at the IBM Passport Advantage website.

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 1 on page 7 identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the IBM Security Directory Integrator server.

Table 1. 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.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
PeopleSoft Enterprise	Version 9.0 Version 9.1
PeopleTools Software	Versions 8.50 Version 8.51 Version 8.52
System Administrator Authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*.

You can install the adapter on all platforms that are supported by IBM Tivoli® Directory Integrator 7.1. For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1: Administrator Guide*.

Related concepts

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

Software downloads

Download the software through your account at the IBM Passport Advantage website.

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

Download the software through your account at the IBM Passport Advantage website.

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Governance Identity Manager Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance 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.

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 2. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains files for the adapters. For example, the jars/connectors subdirectory contains the files for the UNIX adapter.	**Windows:**
		• for version 7.1:
		`drive\Program Files \IBM\TDI\V7.1`
		UNIX:
		• for version 7.1:
		`/opt/IBM/TDI/V7.1`

Table 2. Required information to install the adapter (continued)

Required information	Description	Value

Solution Directory	See the *Dispatcher Installation and Configuration Guide*.	**Windows:**
		• for version 7.1:
		`drive\Program Files \IBM\TDI\V7.1\timsol`
		UNIX:
		• for version 7.1:
		`/opt/IBM/TDI/V7.1/ timsol`

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance 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
Download the software through your account at the IBM Passport Advantage website.

Chapter 3. Installing in the Verify Governance Identity Manager virtual appliance

For Verify Governance Identity Manager target management, you can install an IBM Security Verify 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 3. 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 3. 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.

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

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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.

What to do next

After you finish the installing the adapter software, modify the PRG_USR_Profile record. See “Modifying the PRG_USR_PROFILE record” on page 15

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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

Modifying the PRG_USR_PROFILE record

Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Procedure

1. Log in to the PeopleTools Application Designer by using the PeopleTools account of the adapter.
2. From the **File** menu, click **Open**.

   The Open Definition dialog window is displayed.
3. Select **Record** from the Definition drop-down listbox.
4. Type PRG in the **Name** field and click **Open**.

   A list of matching records is displayed in the **Definitions matching selection criteria** pane.
5. Select **PRG_USR_PROFILE** and click the **Open**.

   The record is opened in the Application Designer.
6. From within the **Record Fields** tabbed pane, right-click the **OPRID** table entry and click **View PeopleCode** from the right-click menu.

The PeopleCode window opens.

7. Select **SaveEdit** from the PeopleCode Event drop-down listbox.

   The following PeopleCode is displayed in the PeopleCode edit pane.

```
If %OperatorId <> PRG_USR_PROFILE.OPRID Then
   If %Panel = Panel.PURGE_USR_PROFILE Then
    Warning MsgGet(48, 122, "Select OK to confirm deletion of User Profile or
        select Cancel.")
   End-If;
Else
   Error MsgGet(48, 109, "Message not found.");
End-If;
```

8. Replace the existing PeopleCode with the following code.

```
If %OperatorId <> PRG_USR_PROFILE.OPRID Then
   If %CompIntfcName <> "ENROLE_DELETE" Then
     If %Panel = Panel.PURGE_USR_PROFILE Then
    Warning MsgGet(48, 122, "Select OK to confirm deletion of User Profile or
       select Cancel.")
     End-If;
   End-If
Else
   Error MsgGet(48, 109, "Message not found.");
End-If;
```

9. From the File menu, click **Save** to save the record.

What to do next

Load the PeopleTools Project for IBM Security Verify Governance Identity Manager. See "Loading the PeopleTools Project" on page 17.

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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

Loading the PeopleTools Project

The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

About this task

The PeopleTools Adapter software contains component interfaces in the ENROLE_AGENT subdirectory of these project files:

- PT854_COMPONENT.zip for PeopleTools 8.54
- PT850_COMPONENT.zip for PeopleTools 8.50, PeopleTools 8.51, and PeopleTools 8.52, PeopleTools 8.53

This ENROLE_AGENT subdirectory is imported into the PeopleTools Application Designer as a PeopleTools Project.

Loading the IBM Security Verify Governance Identity Manager PeopleTools project is a two-part procedure.

1. The project must be copied into the PeopleTools system. See “Loading the component interfaces” on page 18.
2. The project security must be set. The following two sections provide detailed procedures on how to load the PeopleTools project for IBM Security Verify Governance Identity Manager. See “Setting the component interface security” on page 19.

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation

If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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_AGENT directory into the PeopleTools Application Designer as a PeopleTools Project.

Procedure

1. From the `PT850_COMPONENT.zip` file, extract ENROLE_AGENT and its contents into a temporary directory on your file system.
2. Log in to the PeopleTools Application Designer in two-tier mode by using the PeopleTools account of the adapter.
   a) Click **Start** > **Programs** > **Peopletools8.5x** > **Configuration Manager**
   b) Select the appropriate database type (for example, if the 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**.
3. Copy the ENROLE_AGENT project.
    a) Log on to the PeopleTools Application Designer.
    b) From the **Tools** menu, select **Copy Project** and then select **From File** from the submenu.

       The Copy Project from File dialog window is displayed.
    c) Browse to the directory where you extracted ENROLE_AGENT.

       ENROLE_AGENT is displayed in the **Projects:** list area.
    d) Ensure that ENROLE_AGENT is highlighted and click **Select**.

       The ENROLE_AGENT project is loaded. A second dialog window is displayed.
    e) Ensure that Component Interfaces is highlighted and click **Copy**.

       The component interfaces are loaded into PeopleTools.
4. Exit the PeopleTools Application Designer.

Related tasks

Setting the component interface security
You must add components to the permissions list to set security for the PeopleTools project.

Setting the component interface security

You must add components to the permissions list to set security for the PeopleTools project.

Procedure

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

```
ENROLE_CCODE
ENROLE_DELETE
ENROLE_LANGS
ENROLE_PERM
ENROLE_ROLES
ENROLE_USERS
ENROLE_OPRALIAS
```

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

What to do next

Obtain and generate the PeopleSoft resource-specific JAR files. See "PeopleSoft resource-specific JAR files" on page 19.

Related tasks

Loading the component interfaces
You must import the ENROLE_AGENT directory into the PeopleTools Application Designer as a PeopleTools Project.

PeopleSoft resource-specific JAR files

The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

To use these functions, the PeopleTools Adapter requires the following JAR files:

CompIntfc.jar
The Java API JAR file for the ENROLE_AGENT 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
To create a psft.jar file:

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. Create the psft.jar file by using the following command on command prompt.

   ```
   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.

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

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
If the adapter is installed correctly, the PeopleSoftConnector.jar file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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

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_AGENT Component Interface project and open all the component interfaces by double-clicking each component interface.
3. From the menu, select **Build** > **PeopleSoft APIs**.
4. From the Build PeopleSoft API Bindings window, select the Java classes **Build** check box and clear the COM Type Library and C Header Files **Build** check boxes.
5. In the Java Classes frame, select the **Build** check box and select the appropriate Component Interfaces from the list.

   You must select the following options from the list and then click **OK**:

- CompIntfc.CompIntfcPropertyInfo
- CompIntfc.CompIntfcPropertyInfoCollection
- PeopleSoft.* (Select all the Component Interfaces that begin with the prefix PeopleSoft)
- CompIntfc.ENROLE_USERS* (Select all the Component Interfaces that begin with the prefix CompIntfc.ENROLE_USERS)
- CompIntfc.ENROLE_ROLES* (Select all the Component Interfaces that begin with the prefix CompIntfc.ENROLE_ROLES)
- CompIntfc.ENROLE_PERM* (Select all the Component Interfaces that begin with the prefix CompIntfc.ENROLE_PERM)
- CompIntfc.ENROLE_LANGS* (Select all the Component Interfaces that begin with the prefix CompIntfc.ENROLE_LANGS)
- CompIntfc.ENROLE_DELETE* (Select all the Component Interfaces that begin with the prefix CompIntfc.ENROLE_DELETE)
- CompIntfc.ENROLE_CCODE* (Select all the Component Interfaces that begin with the prefix CompIntfc.ENROLE_CCODE)
- CompIntfc.ENROLE_OPRALIAS* (Select all the Component Interfaces that begin with the prefix CompIntfc.ENROLE_OPRALIAS)

Note: If you must generate Component Interface Java files for the entire group of Component Interfaces, click **ALL**.

Specify the appropriate file path for the Java files; otherwise, the Java files are generated in the default location, `*PEOPLESOFT_HOME*\web\psjoa`. The Component Interface Java files are generated in the `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.

The following note applies to PeopleTools 8.54.

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.

6. 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) For PeopleTools 8.50, 8.51, 8.52, and 8.53, run the following command.

      ```
      javac -classpath d:\temp\psjoa.jar *.java
      ```

      where, *d:\temp* is a path to the `psjoa.jar` file.

      For PeopleTools 8.54, 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.

7. 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

8. Copy the generated `CompIntfc.jar` file to the *ITDI_HOME*`\jars\3rdParty\others` directory.
9. 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 more than 300 entries need to be retrieved, the PeopleSoft Connector needs to invoke JDBC queries on the PeopleSoft database tables.

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 more than 300 entries need to be retrieved, the PeopleSoft Connector needs to 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.

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 more than 300 entries need to be retrieved, the PeopleSoft Connector needs to invoke JDBC queries on the PeopleSoft database tables.

The path to the *JDBC_driver*`.jar` file for the database that is used by PeopleSoft, must be copied to the *ITDI_HOME*`\jars\3rdParty\others` directory.

The PeopleTools Adapter establishes the connection directly with the database if it finds more than 300 records to be retrieved. The PeopleTools Adapter uses the JDBC Type 4 drivers to retrieve more than 300 records. To establish the connection to the database you need to 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
```

Related concepts

psjoa.jar file

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

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.

Verifying the adapter installation

If the adapter is installed correctly, the PeopleSoftConnector.jar file exists in the specified directory.

Windows operating system

drive:\Program Files\IBM\TDI\V7.1\jars\connectors\

UNIX operating system

/opt/IBM/TDI/V7.1/jars/connectors/

If this installation is to upgrade a connector, then send a request from IBM Security Verify Governance Identity Manager. 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.

PeopleSoft resource-specific JAR files

The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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.

PeopleSoft resource-specific JAR files

The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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 Identity server. Use this option for importing adapter profiles.

Before you begin

- The Identity server is installed and running.
- You have administrator authority on the 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.

About this task

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

The adapter profile definition file is used to create a target profile on the Verify Governance Identity Manager 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 Verify Governance Identity Manager 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 29.
- Create a connector that uses the target profile. See “Adding a connector” on page 30.

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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 Verify Governance Identity Manager 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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project

The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

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

Adding a connector
After you import the adapter profile on the Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager server can communicate with the managed resource.

Before you begin

Complete Importing the adapter profile.

Note: If you migrated from Verify Governance Identity Manager 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 Verify Governance Identity Manager 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 Verify Governance Identity Manager 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 Verify Governance Identity Manager. For more information, see "Enabling connectors" on page 32.

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project

The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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 4. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	“Adding a connector” on page 30.
Ensure that you enabled the appropriate channel modes for the connector.	“Reviewing and setting channel modes for each new connector” on page 34.

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager 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 Verify Governance Identity Manager.

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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 Verify Governance Identity Manager 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 Verify Governance Identity Manager V5.2.3:

1. Log in to the Verify Governance Identity Manager 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 32.

       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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record

Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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 Verify Governance Identity Manager account attributes.

About this task

This task involves an account attribute mapping definition file, which is included in the adapter package.

The file consists of Verify Governance Identity Manager account attributes and their equivalent attributes in the managed target. The file is structured as *<IGI_attribute>* = *<target_attribute>*.

The *<IGI_attribute>* is fixed and must not be modified. Edit only the *<target_attribute>*. Some *<IGI_attribute>* already has a fixed equivalent *<target_attribute>* of `eraccount`.

Some *<IGI_attribute>* do not have a defined *<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 Verify Governance Identity Manager attribute values.

   ```
   [conversion].<target_attribute>.<IGI_attribute> =
   [<target_attribute_value1>=<IGI_attribute_value1>;...;
   <target_attribute_valuen>=<IGI_attribute_valuen>]
   ```

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

   ```
   [conversion.date].erbirthDate.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 Verify Governance Identity Manager product documentation.
6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

Attribute	**Mapped Attribute**
eruid	CODE
erpassword	PASSWORD

   For more information, see *Mapping attributes for a connector* in the IBM Security Verify Governance Identity Manager 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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile

You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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

Deploying the ID type subform

You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

About this task

You must perform this procedure on both WebSphere® and IBM Security Verify Identity. In a clustered environment the subform must be deployed on each WebSphere application server.

Procedure

1. Extract the `opraliastype.zip` file into a temporary folder

   For example, `C:\temp`.

2. Copy the following files from the temporary folder to the `subforms` directory in the IBM Security Verify Identity WebSphere deployment directory.

   The directory locations are:

   For a self service console installation
   WAS_PROFILE_HOME/installedApps/*server*/ITIM.ear/itim_self_service.war/subforms

   For an administrative console installation
   WAS_PROFILE_HOME/installedApps/*server*/ITIM.ear/itim_console.war/subforms

   For Identity Service Center installation
   WAS_PROFILE_HOME/installedApps/*nodeName*/ITIM.ear/isim_isc_subform.war

   Note: *WAS_PROFILE_HOME* is typically `C:\Program Files\IBM\WebSphere\AppServer\profiles` or `opt/IBM/WebSphere/AppServer/profiles`.

   - `opraliastype\opraliastype.jsp`
   - `opraliastype\storeValues.jsp`
   - `opraliastype\opraliasstyle.css`

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

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.

Note: If the following fields on the service form are changed for an existing service, the adapter service on the Tivoli Directory Integrator server needs to be restarted.

- **JDBC driver**

- **JDBC URL**
- **Database user name**
- **Database user password**
- **AL FileSystem Path**
- **Max Connection Count**

On the General Information tab:

Service Name
Specify a name that defines the adapter service on the Identity 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

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

The default URL for the default SDI1 instance is `rmi://localhost:1099/ITDIDispatcher`.

The following table shows the ports that are open in the firewall for every instance that is created. However, usage of these port numbers do not support high availability.

Table 5. Ports

Instance	Ports
SDI1	1199, 1198, 1197, 1196, 1195, 1194
SDI2	2299, 2298, 2297, 2296, 2295, 2294
SDI3	3399, 3398, 3397, 3396, 3395, 3394
SDI4	4499, 4498, 4497, 4496, 4495, 4494
SDI5	5599, 5598, 5597, 5596, 5595, 5594
SDI6	6699, 6698, 6697, 6696, 6695, 6694
SDI7	7799, 7798, 7797, 7796, 7795, 7794
SDI8	8899, 8898, 8897, 8896, 8895, 8894
SDI9	9999, 9998, 9997, 9996, 9995, 9994
SDI10	11099, 11098, 11097, 11096, 11095, 11094

For a high availability implementation, use any of these port numbers.

- 1099
- 2099
- 3099

Owner
Optional: Specify a user as a service owner.

Service prerequisite
Optional: Specify a service that is a prerequisite to this service.

On the PS Connection tab:

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

APP Server port

Specify the port number used to connect to the PeopleTools Application Server. This number is the IP port number on which the PeopleTools Application Server listens for JOLT connections. This value is typically port 9000.

PS APP ID

Specify the name of the PeopleTools account created for the adapter.

APP ID password

Specify a password of the PeopleTools account 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`. See "JDBC type 4 driver JAR file" on page 23 for more information.

JDBC URL

Specify the Web address that is used to connect 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
```

See "JDBC type 4 driver JAR file" on page 23 for more information.

Database user name

Specify the administrator user name that is used to connect 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.

On the Dispatcher Attributes tab:

AL FileSystem Path

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from Identity server. For example, you can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: `c:\Program Files\IBM\TDI\V7.1\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating systems: `/opt/IBM/TDI/V7.1/profiles`.

Disable AL Caching

Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.

Max Connection Count

Specify the maximum number of assembly lines that the dispatcher can execute simultaneously for the service. If you enter `0` in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines that are executed simultaneously for the service.

On the Status and information tab

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

Last status update: Date

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

Last status update: Time
Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status
Specifies the status of the managed resource that the adapter is connected to.

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

Profile version
Specifies the version of the profile that is installed in the Identity server.

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

Dispatcher version
Specifies the version of the Dispatcher.

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

Adapter account
Specifies the account that running the adapter binary file.

Adapter up time: Date
Specifies the date when the adapter started.

Adapter up time: Time
Specifies the time of the date when the adapter started.

Adapter memory usage
Specifies the memory usage for running the adapter.

If the connection fails, follow the instructions in the error message. Also

- Verify the adapter log to ensure that the test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. For example, verify the work station name or the IP address of the managed resource and the port.

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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record

Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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 Identity server.
2. Run a full reconciliation from the Identity 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.

PeopleSoft resource-specific JAR files
The PeopleTools Adapter uses Java APIs to communicate and perform operations such as add, delete, modify, and search on the PeopleSoft resource.

Verifying the adapter installation
If the adapter is installed correctly, the `PeopleSoftConnector.jar` file exists in the specified directory.

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.

Modifying the PRG_USR_PROFILE record
Use the PeopleSoft Application Designer to modify PRG_USER_PROFILE record.

Loading the PeopleTools Project
The adapter software provides a compressed file that contains the PeopleTools project file. This file provides component interfaces that must be imported into the PeopleTools Application Designer.

Importing the adapter profile
You can import a profile definition file, which creates a profile in Identity 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 Verify Governance Identity Manager server, add a connector so that Verify Governance Identity Manager 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 Verify Governance Identity Manager account attributes.

Deploying the ID type subform
You can use subforms to display additional information on the service form. Use this procedure to enable the use of subforms.

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.

To verify the required version of these adapter components, see the adapter release notes.

Upgrading the adapter binaries or connector

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

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

- If the connector version mentioned in the release notes is later than the existing version on your workstation, install the connector.
- If the connector version mentioned in the release notes is the same or earlier than the existing version, do not install the connector.

Note: Stop the dispatcher service before the upgrading the connector and start it again after the upgrade is complete.

Related concepts

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

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

Related tasks

Regenerating the component interface
In some scenario, it might be required to regenerate the component interface while you upgrade the adapter.

Upgrading the dispatcher

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

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

- If the dispatcher version mentioned in the release notes is later than the existing version on your workstation, install the dispatcher.
- If the dispatcher version 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 binaries or connector
The new adapter package might require you to upgrade the connector.

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

Related tasks

Regenerating the component interface

In some scenario, it might be required to regenerate the component interface while you upgrade the adapter.

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 adapter binaries or connector
The new adapter package might require you to upgrade the connector.

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

Related tasks

Regenerating the component interface
In some scenario, it might be required to regenerate the component interface while you upgrade the adapter.

Regenerating the component interface

In some scenario, it might be required to regenerate the component interface while you upgrade the adapter.

About this task

For more information about regenerating the component interface, see "Loading the component interfaces" on page 18.

Related concepts

Upgrading the adapter binaries or connector
The new adapter package might require you to upgrade the connector.

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

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

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 additional configuration options such as:

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

Customizing the adapter profile

To customize the adapter profile, you must modify the PeopleTools Adapter JAR file. You might customize the adapter profile to change the account form or the service form.

About this task

Use the Form Designer or `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file for that adapter. The JAR file is included in the PeopleTools Adapter compressed file that you downloaded from the IBM website.

Note: To modify the adapter schema, see the *Directory Integrator-Based PeopleTools Adapter User Guide*.

The following files are included in the PeopleTools JAR file:

- CustomLabels.properties
- erpt84xrmiservice.xml
- erpt84xuseraccount.xml
- PeopleToolsAdapterALs.xml
- PeopleToolsAddAL.xml
- PeopleToolsDeleteAL.xml
- PeopleToolsModifyAL.xml
- PeopleToolsSearchAL.xml
- PeopleToolsTestAL.xml
- schema.dsml
- service.def

Procedure

1. To edit the JAR file, log on to the workstation where the PeopleTools Adapter is installed.
2. Copy the JAR file into a temporary directory.
3. Extract the contents of the JAR file into the temporary directory by running the following command.

   The following example applies to the PeopleTools Adapter profile. Type the name of the JAR file for your operating system.

   ```
   #cd /tmp
   #jar -xvf PeopleToolsProfile.jar
   ```

The **jar** command extracts the files into the PeopleToolsProfile directory.

4. Edit the file that you want to change.

   After you edit the file, you must import the file into the Identity server for the changes to take effect.
5. To import the file, create a JAR file by using the files in the /tmp directory by running the following commands:

   ```
   #cd /tmp
   #jar -cvf PeopleToolsProfile.jar PeopleToolsProfile
   ```
6. Import the JAR file into the IBM Security Verify Governance Identity Manager application server.
7. Stop and start the Identity server.
8. Restart the adapter service.

Editing adapter profiles on the UNIX or Linux operating system

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character ^M at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the ^M characters. You can also use text editors, such as the **vi** editor, to remove the characters manually.

Example

You can use the **vi** editor to remove the ^M characters. 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.

Password management when restoring accounts

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account. However, in some cases you might not want to be prompted for a password.

How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement. You can set the PeopleTools Adapter to require a new password when the account is restored, if your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password.

In the service.def file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior from the schema.dsml file. Adapter profile components also enable remote services to find out if you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this situation, only some of the accounts being restored might require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

Edit the service.def file to add the new protocol options, for example:

```
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_REQUIRED_ON_RESTORE"<value>true</value>
</property>
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_ALLOWED_ON_RESTORE"<value>false</value>
</property>
```

By adding the two options in the preceding example, you ensure that you are not prompted for a password when an account is restored.

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 Identity server.
2. Run a full reconciliation from the Identity 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.

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

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 6 on page 53 and Table 7 on page 54 contain warnings or errors which might be displayed in the user interface when the PeopleTools Adapter is installed on your system.

Table 6. Specific warning and error messages and actions

Message number	**Message**	**Action**
CTGIMT600E	An error occurred while establishing communication with the IBM Tivoli 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 Tivoli Directory Integrator is correct.
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 specified on the service form of the PeopleSoft Application Server are correct. • Verify that the PeopleSoft administrator user name and password specified on the service form of the PeopleSoft Application Server are correct.
CTGIMT003E	The account already exists.	The user has already been added to the resource. This error might occur if you are attempting to add a user to the managed resource and Tivoli Identity Manager is not synchronized with the resource. To fix this problem, schedule a reconciliation between Tivoli Identity Manager and the resource. See the online help for information about scheduling a reconciliation.
CTGIMT015E	An error occurred while deleting the *username* account because the account does not exist.	This error might occur when you attempt to delete a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The user was created on the resource. • The user was not deleted from the resource. • If the user does not exist on the resource, create the user on the resource and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.
CTGIMT009E	The account *username* cannot be modified because it does not exist.	This error might occur when you attempt to modify a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The user was created on the resource. • The user was not deleted from the resource. • If the user does not exist on the resource, create the user on the resource and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.

Table 7. General warning and error 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 unavailable. Perform the following steps: • Verify that the CompIntfc.jar file (which contains the ENROLE_AGENT Component Interface project classes) is present in the jars subdirectory of the *ITDI_HOME* directory. • Verify that the CompIntfc.jar file contains classes for the required ENROLE_AGENT Component Interface project. • If necessary, add the path of the jars subdirectory to the ITDI CLASSPATH variable.
• A system error occurred while adding an account. The account was not added. • A system error occurred while modifying an account. The account was not changed. • A system error occurred while deleting an account. The account was not deleted. • The search failed due to a system error.	To fix this problem, ensure that: • The CompIntfc.jar and psjoa.jar are present appropriate locations of the Security Directory Integrator. • The ENROLE_AGENT Component Interface project is deployed on the PeopleSoft resource. • The network connection is not slow between the IBM Security Verify Governance Identity Manager and the Security Directory Integrator or the Security Directory Integrator and the managed resource.
• The account was added but some attributes failed. • The account was modified but some attributes failed. • The account was deleted successfully, but additional steps failed.	The account was created, modified, or deleted, but some of the specified attributes in the request were not set. See the list of attributes that failed and the error message that explains why the attribute failed. Correct the errors associated with each attribute and perform the action again **Note:** You might want to review the documentation for the operating system of the managed resource to determine the correct values for some attributes. .

Table 7. General warning and error messages and actions (continued)

Message	Action
• The user cannot be modified because it does not exist. • An error occurred while deleting the account because the account does not exist.	This error might occur when you attempt to modify or delete a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The location specified for the managed resource is correct. • The user was created on the resource. • The user was not deleted from the resource. If the user does not exist on the resource, create the user on the resource and then schedule reconciliation. See the online help for information about scheduling reconciliation.
• Search filter error • Invalid search filter	The filter specified in the search request is not correct. Specify the correct filter and perform the search action again.
The application could not establish a connection to *hostname.*	Ensure that SSH is enabled on the managed resource.
Adapter profile is not displayed in the user interface after installing the profile.	You must stop and restart the Security Directory Integrator server, or wait until the cache times out (up to 10 minutes) for IBM Security Verify Governance 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.

Chapter 8. Uninstalling

To remove an adapter from the 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 Identity server. Depending on the adapter, some of these tasks might not be applicable, or there can be other tasks.

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

Removing the adapter binaries or connector

The adapter installation process also installs the Security Directory Integrator PeopleSoft connector. Therefore, you must remove the `PeopleSoftConnector.jar` file from the IBM Security Directory Integrator.

Procedure

1. Stop the Dispatcher service.
2. Remove the `PeopleSoftConnector.jar` file from the *`ITDI_HOME`*`/jars/connectors` directory.
3. Start the Dispatcher service.

Deleting the adapter profile

Remove the adapter service/target type from the Identity server. Before you delete the adapter profile, ensure that no objects exist on the Identity server that reference the adapter profile.

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

The mandatory attributes for creating an account are:

- User ID
- Symbolic ID

Table 8. Attributes, OIDs, descriptions and corresponding PeopleTools attributes

Attribute name	Description	Required	PeopleTools attribute
ErUid	User ID	Yes	User ID
ErPassword	Password for the user ID	No	Password
ErAccountStatus	Status of the account (suspended or restored)	No	Account Locked Out
ErLastAaccessDate	Last Access Date	No	The attribute is available in the PeopleSoft database, however, it is not available in the PeopleSoft Pure Internet Architecture (PIA) user interface. For more information, see the LASTSIGNONDTTM column in the PSOPRDEFN table of the PeopleSoft database.
erpt84xsymbid	Symbolic ID	Yes	Symbolic ID
erpt84xdescription	Description	No	Description
erpt84xusersupr	User Supervisor	No	Supervising User ID
erpt84xaltid	Alternate User ID	No	Alternate User ID
erpt84xcurrcode	Currency Code	No	Currency Code
erpt84xemailadd	Email Addresses	No	Edit Email Addresses
erpt84xenddate	To Date	No	To Date
erpt84xlangcode	Language Code	No	Language Code

Table 8. Attributes, OIDs, descriptions and corresponding PeopleTools attributes (continued)

Attribute name	Description	Required	PeopleTools attribute
erpt84xmultilang	Multi Language Enabled?	No	Multiple Language **Note:** The attribute is available in the PeopleSoft database, however, it is not available in the PeopleSoft Pure Internet Architecture (PIA) user interface.
erpt84xhomepagepl	Navigator Homepage	No	Navigator Homepage
erpt84xopraliastype	ID Types and Values	No	ID Type
erpt84xprimarypl	Primary	No	Primary
erpt84xprofilepl	Process Profile	No	Process Profile
erpt84xrole	Roles	No	Roles
erpt84xrowpl	Row Security	No	Row Security
erpt84xstartdate	Effective Date	No	From Date
erpt84xexpertentry	Enable Expert Entry?	No	Enable Expert Entry
erpt84xemailuser	Routing- Email User	No	Email User
erpt84xworklistuser	Routing- Worklist User	No	Worklist user

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.

The lists include more information about required and optional attributes sent to the adapter to complete that action.

System Login Add

A System Login Add is a request to create a new user account with the specified attributes.

Table 9. Add request attributes for AIX®, HPUX, Linux, and Solaris

Required attribute	Optional attribute
erUid erpt84xsymbid	All other supported attributes

Related concepts

System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

System Login Delete
A System Login Delete is a request to remove the specified user from the directory.

System Login Suspend

A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

System Change Password
A System Change Password is a request to change the password of a user.

Test
The following table identifies attributes needed to test the connection.

Reconciliation
The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

System Login Change

A System Login Change is a request to change one or more attributes for the specified users.

Table 10. Change request attributes

Required attribute	**Optional attribute**
erUid	All other supported attributes

Related concepts

System Login Add
A System Login Add is a request to create a new user account with the specified attributes.

System Login Delete
A System Login Delete is a request to remove the specified user from the directory.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

System Change Password
A System Change Password is a request to change the password of a user.

Test
The following table identifies attributes needed to test the connection.

Reconciliation
The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

System Login Delete

A System Login Delete is a request to remove the specified user from the directory.

Table 11. Delete request attributes

Required attribute	**Optional attribute**
erUid	None

Related concepts

System Login Add
A System Login Add is a request to create a new user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

System Change Password
A System Change Password is a request to change the password of a user.

Test
The following table identifies attributes needed to test the connection.

Reconciliation
The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

System Login Suspend

A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

Table 12. Suspend request attributes

Required attribute	Optional attribute
erUid erAccountStatus	None

Related concepts

System Login Add
A System Login Add is a request to create a new user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

System Login Delete
A System Login Delete is a request to remove the specified user from the directory.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

System Change Password
A System Change Password is a request to change the password of a user.

Test
The following table identifies attributes needed to test the connection.

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

System Login Restore

A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

Table 13. Restore request attributes

Required attribute	Optional attribute
erUid erAccountStatus erPassword	None

Related concepts

System Login Add
A System Login Add is a request to create a new user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

System Login Delete
A System Login Delete is a request to remove the specified user from the directory.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

System Change Password
A System Change Password is a request to change the password of a user.

Test
The following table identifies attributes needed to test the connection.

Reconciliation
The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

System Change Password

A System Change Password is a request to change the password of a user.

Table 14. System change password request attributes

Required attribute	Optional attribute
erUid erPassword	None

Related concepts

System Login Add
A System Login Add is a request to create a new user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

System Login Delete

A System Login Delete is a request to remove the specified user from the directory.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

Test
The following table identifies attributes needed to test the connection.

Reconciliation
The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

Test

The following table identifies attributes needed to test the connection.

Table 15. Test attributes

Required attribute	**Optional attribute**
None	None

Related concepts

System Login Add
A System Login Add is a request to create a new user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

System Login Delete
A System Login Delete is a request to remove the specified user from the directory.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

System Change Password
A System Change Password is a request to change the password of a user.

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

Table 16. Reconciliation request attributes

Required attribute	Optional attribute
None	All other supported attributes

Related concepts

System Login Add
A System Login Add is a request to create a new user account with the specified attributes.

System Login Change
A System Login Change is a request to change one or more attributes for the specified users.

System Login Delete
A System Login Delete is a request to remove the specified user from the directory.

System Login Suspend
A System Login Suspend is a request to disable a user account. The user is neither removed nor are their attributes modified.

System Login Restore
A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as those before the Suspend function was called.

System Change Password
A System Change Password is a request to change the password of a user.

Test
The following table identifies attributes needed to test the connection.

Index