IBM Security Verify Governance Identity Manager

SAP NetWeaver Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The SAP NetWeaver Adapter uses the functionality of Security Directory Integrator to enable communication between the Identity server and the SAP NetWeaver Application Server ABAP 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

The adapter automates several administrative and management tasks.

- Creating users and groups
- Modifying users' attributes
- Changing user account passwords
- Suspending, restoring, and deleting user accounts
- Reconciling users and user attributes

In some cases, the standard features and functionality of SAP may not satisfy business requirements. The adapter supports configurable extension and customization for you to map the adapter to your desired requirements. The primary mechanism enabling this is XSL stylesheets, which can be installed with the adapter.

Related concepts

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

Supported configurations
The adapter supports both single and multiple server configurations.

Architecture

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

Identity server communicates with the SAP NetWeaver Adapter to manage SAP NetWeaver AS ABAP user accounts.

You can perform the following actions on an account:

- Add
- Change Password
- Delete
- Modify
- Restore
- Search
- Suspend

The SAP NetWeaver Adapter consists of Security Directory Integrator AssemblyLines. When an initial request is made by Identity server to the adapter, the AssemblyLines are loaded into the Identity server. As a result, subsequent service requests do not require those same AssemblyLines to be reloaded.

The AssemblyLines use the Security Directory Integrator SAP User connector and RFC functional component to enable user management-related tasks on the SAP NetWeaver AS ABAP. It does this enablement remotely by using the login ID and password of a user that has administrator privileges.

The following figure describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

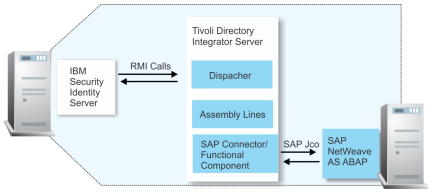

Figure 1. The architecture of the SAP NetWeaver Adapter

Related concepts

Features
The adapter automates several administrative and management tasks.

Supported configurations
The adapter supports both single and multiple server configurations.

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components of the SAP NetWeaver Adapter environment are:

- An Identity server
- An IBM Security Directory Integrator
- The SAP NetWeaver Adapter

Forming part of each configuration, the SAP NetWeaver Adapter must physically reside on the machine that is running the IBM Security Directory Integrator Server.

The SAP Java™ Connector (JCo) component must also be installed on the same Java Runtime Environment (JRE) as used by IBM Security Directory Integrator. See the appropriate SAP JCo guides for instructions on how to install and configure the SAP JCo Runtime Environment.

Single server configuration

In a single server configuration, install the Identity server, the IBM Security Directory Integrator server, and the SAP NetWeaver Adapter on one server to establish communication with the SAP NetWeaver Application Server ABAP server. The SAP NetWeaver Application Server ABAP server is installed on a different server as described Figure 2 on page 3.

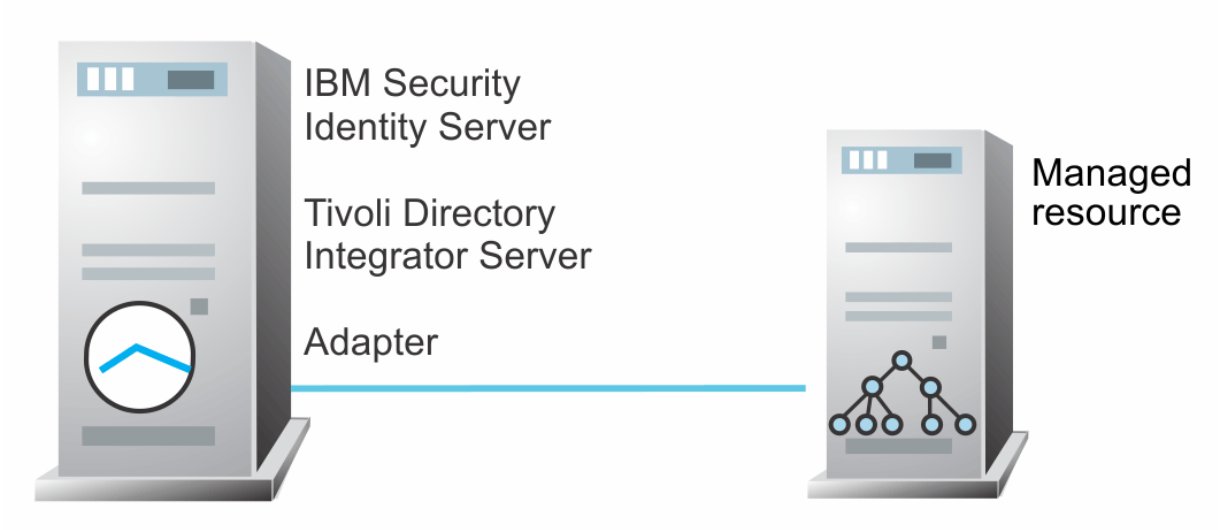

Figure 2. Example of a single server configuration

Multiple server configuration

In multiple server configuration, the Identity server, the SAP NetWeaver Adapter, and the SAP NetWeaver Application Server ABAP server are installed on different servers. Install the IBM Security Directory Integrator server and the SAP NetWeaver Adapter on the same server as described Figure 3 on page 3.

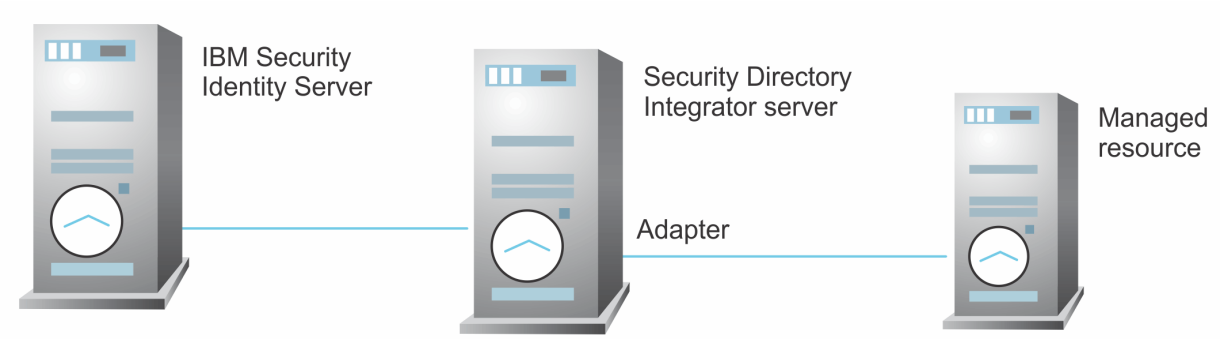

Figure 3. Example of multiple server configuration

The SAP NetWeaver Adapter is both highly configurable and highly customizable. Note that support can only extend to the configuration of the adapter such as adding mapping for additional attributes and XSL stylesheets. Support cannot extend to customization by way of changes, additions or modifications to its IBM Security Directory Integrator Assembly Line scripts for example.

Related concepts

Features

The adapter automates several administrative and management tasks.

Architecture

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

Chapter 2. Planning

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

Use the Preinstallation roadmap to prepare the environment.

Table 1. Preinstallation road map	
Task	**For more information, see**
Verify that your environment meets the software and hardware requirements for the adapter.	“Prerequisites” on page 11.
Obtain the installation software.	Software download.
Obtain the necessary information for the installation and configuration.	“Installation worksheet” on page 13.

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

Table 2. Installation and configuration roadmap	
Task	**For more information, see**
Install the dispatcher.	“Installing the dispatcher” on page 18.
Install the adapter style sheets	“Installing the adapter style sheets” on page 20
Install the adapter JAR files	“Installing the adapter binaries or connector” on page 22
Install the connector.	• “ Installing the SAP Java Connector (JCo)” on page 24 • “Enabling the SAP Java Connector (JCo) trace” on page 27
Enable Unicode	“ Enabling Unicode” on page 32
Verify the adapter installation.	“Verifying the adapter installation” on page 37
Import the adapter profile into the Identity server.	Importing the adapter profile.
Create an adapter service.	Creating an adapter service.
Test the connection.	“Connection test” on page 88
Configure the adapter.	configuration.

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

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

Pre-installation

Complete these tasks.

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

2. Obtain the installation software. See *Software downloads*.
3. Obtain the necessary information for the installation and configuration. See *Installation worksheet*.

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the 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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the 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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

1. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.

7. Create an adapter service/target.
8. Install the adapter language package.
9. Verify that the adapter is working correctly.

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the 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

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

Prerequisites

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

Table 3 on page 11 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 3. Prerequisites to install the adapter

Prerequisite	**Description**
Operating System	The SAP NetWeaver Adapter can be used on any operating system that is supported by Security Directory Integrator.
Network Connectivity	TCP/IP network
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.

Table 3. Prerequisites to install the adapter (continued)	
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
Dispatcher	For Security Directory Integrator Server 7.1, obtain the dispatcher installer from the IBM Passport Advantage® Web site: http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
SAP NetWeaver Application Server ABAP with SAP Basis Component	See the *Adapter for SAP NetWeaver AS ABAP Release Notes®*.
SAP JCo	3.0.9

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1: Administrator Guide*.

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 IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

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

Table 4. Required information to install the adapter

Required information	Description
Administrator account on the managed resource for running the SAP NetWeaver Adapter.	**Note:** Ensure that the adapter user is granted access to SNC. An administrator account on the managed resource that has administrative rights. For example, you want to manage `Resource1` and the SAP NetWeaver Adapter is installed on `Resource1`, then `Admin1` account must have a **Role** containing the following SAP authorization objects: • S_RFC • S_RFCACL • S_TABU_DIS • S_USER_GRP • S_USER_AGR • S_USER_PRO • S_USER_SYS

Chapter 3. Installing

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

Pre-installation tasks

Before you install the adapter, ensure that you complete the preliminary tasks.

- Verify that your site meets all the prerequisite requirements.
- Obtain a copy of the installation software.
- Obtain system administrator authority.

You must also perform the following tasks:

Download the SAP Java Connector (JCo)

The adapter requires access to the SAP Java Connector (JCo) API at run time. This API must be downloaded from the SAP support portal.

Access to this website requires authentication with a valid SAP support ID (S-ID). Contact your SAP marketing representative to obtain one of these IDs.

Check JCo dependencies in current Security Directory Integrator environment

The adapter supports JCo 3.0.9, 3.0.11 and 3.0.12. The version of JCo used by the adapter is updated to 3.0.x.x. The adapter no longer works with JCo 2.1.x. If the adapter is used in the same Security Directory Integrator JVM instance as the SAP connectors that are provided with Security Directory Integrator, you need to have both 3.0.x.x and 2.1.x versions of the JCo installed. If the adapter is used in a single Security Directory Integrator JVM instance, remove the existing JCO 2.1.x package and then install the JCo 3.0.x.x package.

Remove JCo 2.1.x from Security Directory Integrator

If there are no dependencies on an earlier version of JCo such as Version 2.1.8 by other connectors in the Security Directory Integrator environment, the following files can be removed.

Windows

```
ITDI_HOME/jars/3rdparty/others/sapjco.jar
ITDI_HOME/libs/sapjcorfc.dll
ITDI_HOME/libs/librfc32.dll
```

Unix/Linux

```
ITDI_HOME/jars/3rdparty/others/sapjco.jar
```

Create a SAP Service User Account on the target SAP NetWeaver Application Server ABAP

The adapter requires a service account on the target SAP NetWeaver Application Server ABAP to perform account provisioning operations. Log on to the target SAP NetWeaver Application Server ABAP. Create a user account of type “SERVICE”, which can be used by the adapter when it is communicating with SAP.

The SAP user account that is used by IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager to connect to your SAP system must have authorization to perform the following user administration tasks:

1. Add, Modify, Delete, Lock, Unlock, and Search SAP user accounts.
2. Retrieve supporting data through the SAP system database tables.

At a minimum, this account requires assignment of roles that contain the following SAP authorization objects:

- S_RFC

- S_RFCACL
- S_TABU_DIS
- S_USER_GRP
- S_USER_AGR
- S_USER_PRO
- S_USER_SYS
- P_ORGIN(If HR linking extensions are used)

Within the Authorization Objects, assign the wildcard "*" so that all Activities are possible.

CUA Configuration settings

If the adapter is to be deployed against a CUA master server, use transaction SCUM on the target CUA master system to set the following distribution parameters.

- Logon data -> Initial password == "Everywhere"
- Lock -> Unlock globally == "Global"
- Lock -> Lock globally == "Global"

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

Creating an adapter service/target

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

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

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

Installing the 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

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

Creating an adapter service/target

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

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

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

Installing the adapter style sheets

The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

About this task

The adapter style sheets must be copied from the SAP NetWeaver Adapter package to an `xsl` directory as follows:

Procedure

1. If the Dispatcher is installed on *solution* directory (for example, `timsol`), navigate to that directory. Otherwise, navigate to the *ITDI_HOME* directory.
2. Create a directory with the name `xsl`, if one does not already exist.
3. Copy the files from the `tdi/xsl` directory of the adapter package to the `xsl` directory of the IBM Security Directory Integrator *solution* directory, or *ITDI_HOME* directory, depending on your Dispatcher installation.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package

The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Installing the adapter binaries or connector

The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

About this task

These are specific to the SAP NetWeaver Adapter, not general-purpose IBM Security Directory Integrator components. Install these components as follows:

Procedure

1. Copy `tdi/connectors/*.jar` from the adapter package to the *ITDI_HOME*`/jars/connectors` directory.
2. Copy `tdi/functions/*.jar` from the adapter package to the *ITDI_HOME*`/jars/functions` directory.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Installing the SAP Java Connector (JCo)

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. After you download the JCo package, unpack the contents and then follow these instructions.

About this task

The SAP NetWeaver Adapter is tested and certified by using Java Connector, version 3.0.13. It is the same JCo version that SAP made available at the time when this adapter was released.

Note: SAP might release a newer version of JCo before the next release of the adapter and might remove JCo version 3.0.13 from download. The newer version of JCo might work as is with the adapter. If there are any issues that are related directly to the newer version of JCo, it will be addressed in the next release of the adapter.

Procedure

- **Windows:**
  a) Copy the `sapjco3.jar` file into *ITDI_HOME*`/jars/3rdparty/others`.
  b) Copy the `sapjco3.dll` file into *ITDI_HOME*`/libs`.
     On Windows, JCo 3 requires additional Microsoft Visual C++ 2005 libraries to be installed. Installation details for the package that contains these libraries are specified in Microsoft Knowledge Base article 973544.
  c) Restart the adapter service.
- **UNIX or Linux:**
  a) Create a symbolic link to the `sapjco3.jar` file in *ITDI_HOME*`/jars/3rdparty/others`:

```
ln -s <sapjco_install_dir>/sapjco3.jar
   ITDI_HOME/jars/3rdparty/others/sapjco3.jar
```

b) Add the SAP JCo installation directory to the dynamic library path:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<sapjco_install_dir>
export LIBPATH=$LIBPATH:<sapjco_install_dir>
```

c) Restart the Dispatcher.

For assistance, see "Restarting the adapter service" on page 40.

Note: These steps ensure that the sapjco3 libraries are included in the executable path and in the loadable library path, when required. The environment variable for dynamic library path and the command for restarting the Dispatcher might vary on different UNIX operation systems.

- **Linux on System z 64-bit architecture (s390x)**

a) Create a symbolic link to the `sapjco3.jar` file in *ITDI_HOME*`/jars/3rdparty/others`:

```
ln -s <sapjco_install_dir>/sapjco3.jar
   ITDI_HOME/jars/3rdparty/others/sapjco3.jar
```

b) Add the SAP JCo installation directory to the dynamic library path:

```
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:<sapjco_install_dir>
export LIBPATH=$LIBPATH:<sapjco_install_dir>
```

c) SAP JCo is supported on Linux on System z only for 64-bit architecture. The IBM Security Directory Integrator is packaged only with the 31-bit version of Java. Additionally, it must be configured to run with the 64-bit version of Java.

The following steps change the JVM for the complete IBM Security Directory Integrator instance, not only for the Dispatcher.

a. Stop the Dispatcher:

```
/etc/init.d/ITIMAd stop
```

b. Install the IBM Java 1.5 64-bit release (for example `ibm-java2-s390x-5.0.9.rpm`)

d) Change the IBM Security Directory Integrator JRE to become 64 bit:

```
mv  ITDI_HOME/jvm/jre ITDI_HOME/jvm/jre32
ln -s JAVA_1.5_64BIT_HOME/jre ITDI_HOME/jvm/jre
```

e) Start the Dispatcher:

```
/etc/init.d/ITIMAd start
```

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation

After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Enabling the SAP Java Connector (JCo) trace

Activate traces to get more information that can help you analyze errors that are related to connection issues.

Procedure

1. Navigate to the IBM Security Directory Integrator adapters solution directory.
   For example, *ITDI_HOME*\timsol.
2. Open the file in an editor.

   For Windows operating systems
   Open the file ibmdiservice.props

   For UNIX or Linux operating systems
   Open the file ibmdisrv
3. Edit the following property:

   - For Windows operating systems

     ```
     jvmcmdoptions=-Djco.trace_level=10 -Djco.trace_path=E:\jco_trace\ -Djco.rfc=1
     ```

     Where:

     -Djco.trace_level=N
     The trace level can be 0 - 10, where 10 being the most detailed trace.

-Djco.trace_path=<PATH>
If a trace path is set, the JCo traces are written to one or multiple files that are named JCO*<date>*_*<time>*.*<no>*.trc in the specified PATH directory. Otherwise, the JCo traces are written to the standard output stream, where, by default is an output to the console.

Note: The jco_trace directory must be available.

-Djco.jrfc=1
If set to 1, JCo trace is enabled for all connections. This configuration should be the last resort.

- For UNIX or Linux operating systems

```
-Djco.trace_level=10 -Djco.trace_path=/opt/jco_trace/ -Djco.rfc=1
```

Where:

-Djco.trace_level=N
The trace level can either be 0 or 10, where 10 being the most detailed trace.

-Djco.trace_path=<PATH>
If a trace path is set, the JCo traces are written to one or multiple files that are named JCO*<date>*_*<time>*.*<no>*.trc in the specified PATH directory. Otherwise, the JCo traces are written to the standard output stream, where, by default is an output to the console.

Note: The jco_trace directory must be available.

-Djco.jrfc=1
If set to 1, JCo trace is enabled for all connections. This configuration should be the last resort.

For example:

```
"%TDI_JAVA_PROGRAM%"  -Xdebug -Xnoagent -Djava.compiler=NONE -Djco.trace_level=10
 -Djco.trace_path=/opt/jco_trace/ -Djco.rfc=1
-Xrunjdwp:transport=dt_socket,server=y,suspend=n,address=5555 -classpath
"%TDI_HOME_DIR%\IDILoader.jar" %ENV_VARIABLES% com.ibm.di.loader.ServerLauncher %*
set RC=%ERRORLEVEL%
```

4. Save your changes.
5. Restart the adapter service.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: SapNWProfile.jar and SapGRCNWProfile.jar.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Adapter profile

There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

The difference between the two profiles is that the `SapGRCNWProfile.jar` contains additional attributes that allow the adapter to be configured with either SAP GRC Access Control 5.3 or SAP GRC Access Control 10.0.

If only the SAP NetWeaver Adapter is to be used, then use `SapNWProfile.jar`.

If SAP GRC is to be used as part of the SAP NetWeaver account provisioning process, then use `SapGRCNWProfile.jar`.

If IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager contains an existing SAP NW profile and the SAP NW GRC profile is to be imported, the SAP NW GRC profile will overwrite the SAP NW profile. The SAP NW GRC profile contains both the SAP GRC attributes and the SAP NW attributes in the one profile. It is not possible for both a SAP NW profile and SAP NW GRC profile to exist in the same IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager instance.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Enabling Unicode

To support multibyte character encoding, you must configure the Dispatcher JVM properties.

About this task

The Dispatcher process is a running instance of the IBM Security Directory Integrator server.

The IBM Security Directory Integrator is a Java application that is running its own JVM. You can supply standard JVM properties to the Dispatcher such as:

- Encoding
- Memory allocation initial size
- Memory allocation maximum size

As an example, to set up the dispatcher encoding to UTF-8, perform the following steps:

Procedure

- **On Windows operating systems**
  a) Stop the IBM Security Directory Integrator (Security Adapters) service.
  b) Navigate to the adapter *timsol* directory.
  c) Open the `ibmdiservice.props` file with a text editor.
  d) Set the value of the `jvmcmdoptions` property to the Java property value that you want to change to.

For example, if you want the Dispatcher JVM to run with UTF-8 encoding, then set `jvmcmdoptions=- Dfile.encoding=UTF-8`.

Note: When you set multiple properties, separate two properties with a space.

e) Save and close the `ibmdiservice.props` file.

f) Start the IBM Security Directory Integrator (Security Adapters) service.

- **On UNIX or Linux® operating systems**

a) Navigate to the *ITDI_HOME* installation directory.

b) Run the following command:

```
vi ibmdisrv
```

c) Modify the string value in the following format:

```
"$JRE_PATH/java" -cp "/opt/IBM/TDI/V7.1/jars/3rdparty/IBM/
db2jcc_license_c.jar" "-Dlog4j.configuration=file:etc/
log4j.properties" -jar "/opt/IBM/TDI/V7.1/IDILoader.jar"
com.ibm.di.server.RS "$@"
```

For example, if you want the JVM to use UTF-8 encoding, then modify the command as:

```
"$JRE_PATH/java" -cp "/opt/IBM/TDI/V7.1/jars/3rdparty/IBM/
db2jcc_license_c.jar" "-Dfile.encoding=UTF-8" "
-Dlog4j.configuration=file:etc/log4j.properties" -jar
"/opt/IBM/TDI/V7.1/IDILoader.jar" com.ibm.di.server.RS "$@"
```

d) Restart the dispatcher service. Run one of the following commands to restart the process:

– On AIX® operating systems:

```
/opt/IBM/TDI/V7.1/timsol/ITIMAd restartsrc
```

– On Linux, Solaris, and HP-UX operating systems:

```
/opt/IBM/TDI/V7.1/timsol/ITIMAd restart
```

- **Enabling UTF-8 encoding for the Dispatcher and adapter log file is suggested.**

Logging capabilities are provided by IBM Security Directory Integrator. Encoding settings can be enabled as follows:

a) Open the file `ITDI_HOME/`*`solution`*`/etc/log4j.properties` in a text editor.

b) After the line `log4j.appender.Default.file=logs/ibmdi.log`, add the following setting:

```
log4j.appender.Default.file.encoding=UTF-8
```

c) The resulting entry looks like the following example:

```
log4j.appender.Default=org.apache.log4j.FileAppender
log4j.appender.Default.file=logs/ibmdi.log
log4j.appender.Default.file.encoding=UTF8
log4j.appender.Default.layout=org.apache.log4j.PatternLayout
log4j.appender.Default.layout.ConversionPattern=%d{ISO8601} %-5p [%c] - %m%n
log4j.appender.Default.append=false
```

d) Restart the adapter service.

Related concepts

Pre-installation tasks

Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

CUA configuration settings

If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

You must set the following distribution parameters:

- Logon data -> Initial password == "Everywhere"
- Lock -> Unlock globally == "Global"
- Lock -> Lock globally == "Global"

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Verifying the adapter installation

After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

These adapter components must exist on the IBM Security Directory Integrator server.

Table 5. Adapter components

Directory	**Adapter component**
ITDI_HOME/jars/connectors	SapNWUserConnector.jar, SapNWSupport.jar
ITDI_HOME/jars/functions	SapNWRfc.jar
ITDI_HOME/jars/3rdparty/other	sapjco3.jar

Table 5. Adapter components (continued)	
Directory	**Adapter component**
ITDI_HOME/libs	sapjco3.dll
ITDI_HOME/solution/xsl	• sapnw_bapi_errors.properties • sapnw_bapi_user_actgroups_assign.xsl • sapnw_bapi_user_actgroups_delete.xsl • sapnw_bapi_user_change.xsl • sapnw_bapi_user_change_licensedata.xsl • sapnw_bapi_user_create.xsl • sapnw_bapi_user_delete.xsl • sapnw_bapi_user_disablepassword.xsl • sapnw_bapi_user_getdetail_postcall.xsl • sapnw_bapi_user_getdetail_precall.xsl • sapnw_bapi_user_getlist_postcall.xsl • sapnw_bapi_user_getlist_precall.xsl • sapnw_bapi_user_locactgroups_assign.xsl • sapnw_bapi_user_locactgroups_read_postcall.xsl • sapnw_bapi_user_locactgroups_read_precall.xsl • sapnw_bapi_user_lock.xsl • sapnw_bapi_user_locprofiles_assign.xsl • sapnw_bapi_user_locprofiles_read_postcall.xsl • sapnw_bapi_user_locprofiles_read_precall.xsl • sapnw_bapi_user_profiles_assign.xsl • sapnw_bapi_user_profiles_delete.xsl • sapnw_bapi_user_system_assign.xsl • sapnw_bapi_user_unlock.xsl

If the adapter is installed correctly, these dispatcher components exist on the IBM Security Directory Integrator server.

If this installation is to upgrade a connector, send a request from IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager and verify that the version number in the ibmdi.log matches the version of the connector.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings

If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

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

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

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings

If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Importing the adapter profile

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

Before you begin

- The Identity server is installed and running.
- You have root or 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.The JAR file for IBM Security Identity Manager is located in the top level folder of the installation package.

About this task

Service definition files are also called adapter profile files.

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:
   a) In the **Service Definition File** field, type the directory location of the <*Adapter*>`Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the AD`ProfileJAR` file.
   b) Click **OK** to import the file.

Results

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

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the **`handler.file.fileDir`** property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server*HOME*`\data` directory. .

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test

After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Importing the adapter profile

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

Before you begin

- You have root or 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.The JAR file for IBM Security Identity Manager is located in the top level folder of the installation package.

About this task

Service definition files are also called adapter profile files.

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

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:

   a) In the **Service Definition File** field, type the directory location of the `<Adapter>Profile.jar` file, or click **Browse** to locate the file.

For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.

b) Click **OK** to import the file.

Results

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

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the **`handler.file.fileDir`** property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server*HOME*`\data` directory. .

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)

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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

Creating an adapter service/target

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

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

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

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

Procedure

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

Results

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

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage**

Service Types page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.

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

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

Importing the adapter profile

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Verifying that the adapter is working correctly

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

Importing the adapter profile

You can import a profile definition file, which creates a profile in 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 54.
- Create a connector that uses the target profile. See "Adding a connector" on page 56.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode

To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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

Adding a connector
After you import the adapter profile on the 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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Verifying that the adapter is working correctly

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

Importing attribute mapping file

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

About this task

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

Procedure

1. Log in to the 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

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test

After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Adding a connector

After you import the adapter profile on the 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 59.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets

The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Creating an adapter service/target

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

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

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

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

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

Enabling connectors

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

Before you begin

Table 6. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 56.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 62.

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

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace

Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Verifying that the adapter is working correctly

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

Reviewing and setting channel modes for each new connector

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

About this task

Note: Legacy 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 59.

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

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace

Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Verifying that the adapter is working correctly

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the 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

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

Importing the adapter profile

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

About this task

The complex attribute handler enables IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager to define accesses on service groups that

require additional values when assigned to an account. The access will be defined on the group name only, and the complex attribute handler will internally supply the default values that are needed for the composition value sent to the adapter.

For the SAP Adapter, Versions 6.0.20, 7.0.20, and later, you can expose an SAP role as an access.

The complex attribute handler is provided as a Java class jar file that must be deployed on the IBM Security Verify Identity server. The minimum IBM Security Verify Identity version level required is IBM Security Verify Identity, Version 6.0 Fix Pack 11.

Procedure

1. Extract the complex handler jar file, `SAPHandler.jar`, from the adapter package.
2. Copy the complex handler jar file to `ITIM_HOME/lib`.
3. Add the complex handler jar file to the WebSphere® Application Server shared libraries.
   a) From the WebSphere Application Server Administrative Console., navigate to **Environment** > **Shared libraries** > **ITIM_LIB**.
   b) Add `${ITIM_HOME}/lib/SAPHandler.jar` under the class path as follows:

```
${ITIM_HOME}/lib/SAPHandler.jar
${ITIM_HOME}/lib/itim_util.jar
```

4. Restart the WebSphere Application Server.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets

The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

Creating an adapter service/target

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

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

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

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

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

About this task

The complex attribute handler enables IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager to define accesses on service groups that require additional values when assigned to an account. The access will be defined on the group name only, and the complex attribute handler will internally supply the default values that are needed for the composition value sent to the adapter.

For the SAP Adapter, Versions 6.0.20, 7.0.20, and later, you can expose an SAP role as an access.

The complex attribute handler is provided as a Java class jar file that must be deployed on the IBM Security Verify Identity server. The minimum IBM Security Verify Identity version level required is IBM Security Verify Identity, Version 7.0.1 Fix Pack 1.

Procedure

1. From the top-level menu of the Appliance Dashboard, navigate to **Configure** > **Advanced Configuration** > **External Library**.
2. Select **New** to open the **Add External Library** window.
3. Browse to upload the SAP`Handler.jar` file.
4. Click **Save Configuration** to complete this task.
5. From **Server Control Menu**, select **Security Identity Manager Server** > **Restart**.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation

After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Creating an adapter service/target

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

Before you begin

Complete “Importing the adapter profile” on page 42.

About this task

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

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

Procedure

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

4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.
      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
   If the table contains multiple pages, you can do the following tasks:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:
   ```
   <Domain Name>\<Login Name>
   ```
8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.
   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.
    Specify the expected access information and any other optional information such as description, search terms, more information, or badges.
11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.
    The adapter must be running to obtain the information.
12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.
    The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.
    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.
13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.
    The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.
    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.
14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

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

Results

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

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

Importing the adapter profile

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

Verifying that the adapter is working correctly

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

Creating an adapter service/target

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

Before you begin

Complete "Importing the adapter profile" on page 45.

About this task

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

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

Procedure

1. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.
      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.
   If the table contains multiple pages, you can do the following tasks:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

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

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

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

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

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

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

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

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

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.
14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

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

Results

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

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Creating an adapter service/target

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

Before you begin

Complete “Importing the adapter profile” on page 48.

About this task

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

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

Procedure

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

a) Type information about the business unit in the **Search information** field.

b) Select a business type from the **Search by** list, and then click **Search**.

A list of business units that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.

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

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

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

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

Results

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

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package

The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Service/Target form details

Complete the service/target form fields.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

Creating an adapter service/target

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

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

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

ADAPTER DETAILS TAB

This tab describes service details.

Service name
Specify a name that defines this service on the Identity server.

Note: Slash (/) and backslash (\) characters are not allowed in the service name.

Description
Optional: Specify a description for this service.

IBM Security Directory Integrator location
Optional: Specify the URL for the IBM Security Directory Integrator instance. Valid syntax is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the IBM Security Directory Integrator host and *port* is the port number for the Dispatcher. For example, you might specify the URL as `rmi://localhost:1099/ITDIDispatcher`. For information about changing the port number, see the *Dispatcher Installation and Configuration Guide*.

Service prerequisite
Prerequisite services names.

Owner
Service owner.

SAP CONNECTION DETAILS TAB

This tab describes connection details.

Target Client
The SAP instance client number. This field is mandatory if no value is supplied for **Optional RFC Connection Parameters**.

Login ID
The SAP User account login ID that adapter uses to connect to the SAP instance. This field is mandatory if no value is supplied for **Optional RFC Connection Parameters**.

Password
Password for SAP User account. This field is mandatory if no value is supplied for **Optional RFC Connection Parameters**.

SAP System (DNS hostname or IP)
Host name of the SAP server host computer only if DNS is set up correctly. Otherwise, use the IP address. This field is mandatory if no value is supplied for **Optional RFC Connection Parameters**.

SAP Systems Number
The SAP server system number. This field is mandatory if no value is supplied for **Optional RFC Connection Parameters**.

SAP Logon Language
The language ISO identifier to be used by the adapter. This parameter is optional.

SAP Gateway (DNS hostname or IP)
Host name of the SAP gateway host computer only if DNS is set up correctly. Otherwise, use the IP address. This host is typically the same host that contains the SAP server. This parameter is optional.

Optional RFC Connection Parameters

This attribute allows for alternative SAP connectivity parameters to be specified. The value of this attribute is a formatted string of name-value pairs. Each pair must be separated by a single pipe (|) character. The name parts must be in lowercase characters. The general format of the value of this attribute is shown in this example:

```
<name1>=<value1> <name2=value2> ... <nameN>=<valueN>
```

For example, the following string value would set the SAP Message Server to `messageserver.com` with System ID PR0 and Group SPACE:

```
mshost=messageserver.com|r3name=PR0|group=SPACE
```

The names and values are those supported directly by the SAP RFC API. A summary of the names is supplied in the following table:

Table 7. Names supported by SAP RFC API

Name	**Description**
client	SAP client
user	User name for logon. Set to $MYSAPSS02$ if you are using SSO logon. Set to $X509CERT$ if you are using X509 certificates.
alias user	Alias for user name
passwd	Password of the user. If you are using SSO or X509 certificates, supply base64 encode value of SSO ticket or X509 certificate.
lang	Log on language to be used
sysnr	System number of the target SAP system
ashost	Host name of the target SAP application server
mshost	Host name of message service
gwhost	Host name of the SAP gateway service
gwserv	Gateway service name
r3name	R/3 name
group	Name of SAP application server group
tpname	Program Id of external RFC server program
tphost	Host name of external RFC server program
trace	Set to 1 to enable RFC API trace logging
codepage	SAP code page
getsso2	Set to 1 to obtain SAP SSO ticket
mysapsso2	SAP Cookie version 2 as logon ticket
x509cert	X509 certificate as logon ticket
snc_mode	Set to 1 to enable secure network connection
snc_partnername	SNC name
snc_qop	SNC strength, 1 - 9
snc_myname	SNC name. Overrides partner name

Table 7. Names supported by SAP RFC API (continued)	
Name	**Description**
snc_lib	Path name to SNC library implementation
extiddata	External authentication (PAS) data
extidtype	External authentication type

Type B (Load balancing) connection

The mandatory attributes for Type B connection are `client`, `user`, `passwd`, `lang`, `type`, `mshost`, `r3name`, and `group`.

To establish **Type B (Load Balancing) connection**, add the following value under **Optional RFC Connection Parameters**:

```
type=B|mshost=<Message Server Name>|r3name=<SYSTEM ID>|
group=<Name of SAP application server group>
```

For example: `type=B|mshost=SAPPR0|r3name=PR0|group=SPACE` where message server name is SAPPR0 with systemID as PR0 and group SPACE.

Note:

- The dispatcher must be restarted for each change in the **Optional RFC Connection Parameters?** field.
- To establish a **Type B (Load Balancing) connection**, enable RFC Load balancing in SAP system.

Enable TDI Debugging
Flag to enable IBM Security Directory Integrator debugging trace output.

SAP ROLE DETAILS TAB

This tab describes the role end date.

Role Default End Date : Date/Time
This is the default Role End Date.

ADD ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing add operation requests.

The following attribute of this tab is an optional service attribute. For more details, see Chapter 5, “Configuring,” on page 99.

- Add User Basic XSL Stylesheets

MODIFY ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing modify operation requests.

The following attributes of this tab are all optional service attributes. For more details, see Chapter 5, “Configuring,” on page 99.

- Modify User Basic XSL Stylesheets
- Modify User Basic Lookup Request Stylesheet
- Modify User Basic Lookup Response Stylesheet

DELETE ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing delete operation requests.

The following attributes of this tab are all optional service attributes. For more details, see Chapter 5, “Configuring,” on page 99.

- Delete User Basic XSL Stylesheets
- Delete User Basic Lookup Request Stylesheet
- Delete User Basic Lookup Response Stylesheet

SUSPEND ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing suspend operation requests.

The following attributes of this tab are all optional service attribute.

- Suspend User Basic XSL Stylesheets
- Suspend User Basic Lookup Request Stylesheet
- Suspend User Basic Lookup Response Stylesheet

RESTORE ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing restore operation requests.

The following attributes of this tab are all optional service attribute. For more details, see Chapter 5, “Configuring,” on page 99.

- Restore User Basic XSL Stylesheets
- Restore User Basic Lookup Request Stylesheet
- Restore User Basic Lookup Response Stylesheet

CHANGE PASSWORD ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing password operation requests.

The following attributes of this tab are all optional service attributes. For more details, see Chapter 5, “Configuring,” on page 99.

- Change Password Basic XSL Stylesheets
- Change Password Basic Lookup Request Stylesheet
- Change Password Basic Lookup Response Stylesheet

RECONCILIATION ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing reconciliation and search operation requests.

The following attributes of this tab are all optional service attribute. For more details, see Chapter 5, “Configuring,” on page 99.

- Search User Basic Select Request XSL Stylesheets
- Search User Basic Select Response Stylesheet
- Search User Basic Iterate Request XSL Stylesheets
- Search User Basic Iterate Response Stylesheet

DISPATCHER ATTRIBUTES TAB

This tab describes Dispatcher attributes.

Assembly Line File System Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager. For example, you can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: `C:\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 system: `/opt/IBM/TDI/V7.1/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can execute simultaneously for the service. For example, enter 10 when you want the dispatcher to execute maximum ten assembly lines 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.

Disable Assembly Line Cache
Select the checkbox 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.

Connection test

After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Configuration information for the adapter is reported in the IBM Security Directory Integrator log file (`ibmdi.log`) as a result of a successful test.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets

The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

Installing the adapter language package

The adapters use a separate language package from IBM Security Verify Identity.

See *Installing the adapter language pack* from the IBM Security Verify Identity product documentation.

Related concepts

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Related tasks

Installing the adapter style sheets

The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

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

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

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test

After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler

An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Verifying that the adapter is working correctly

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

Procedure

1. Test the connection for the service that you created on the 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

Pre-installation tasks
Before you install the adapter, ensure that you complete the preliminary tasks.

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.

Adapter profile
There are two adapter profiles included in the SAP NetWeaver Adapter distribution package: `SapNWProfile.jar` and `SapGRCNWProfile.jar`.

CUA configuration settings
If the adapter is to be deployed against a CUA master server, use the transaction SCUM on the target CUA master system to set the distribution parameters.

Verifying the adapter installation
After the adapter is installed, you must verify the adapter components on the IBM Security Directory Integrator server.

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.

Connection test
After the service has been created, click **Test** to ensure that the connection to both IBM Security Directory Integrator Server and SAP NetWeaver AS ABAP can be established.

Installing the adapter language package
The adapters use a separate language package from IBM Security Verify Identity.

Related tasks

Installing the adapter style sheets
The SAP NetWeaver Adapter requires a set of style sheets, which are used by the adapter's IBM Security Directory Integrator assembly lines.

Installing the adapter binaries or connector
The SAP NetWeaver Adapter ships with additional IBM Security Directory Integrator components.

Installing the SAP Java Connector (JCo)
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. After you download the JCo package, unpack the contents and then follow these instructions.

Enabling the SAP Java Connector (JCo) trace
Activate traces to get more information that can help you analyze errors that are related to connection issues.

Enabling Unicode
To support multibyte character encoding, you must configure the Dispatcher JVM properties.

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

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

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

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.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

Installing the Complex Attribute Handler
An account attribute is considered complex when its value is a composition of two or more simple values. The syntax of the composition value is defined by a complex attribute handler that is provided in the adapter package.

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

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

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

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

Chapter 4. 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.

Upgrade of the adapter from version 5.1.4 or older

The version of SAP JCo used by the adapter has been upgraded. See the section about upgrading the SAP JCo for details.

The adapter service configuration forms have changed in the SAP NetWeaver Adapter GUI for XSL advanced mapping. The CUA and NON-CUA specific advanced mappings for Add and Modify operations have been removed.

The following Add Advanced Mapping options have been removed:

- Add User CUA XSL Stylesheets (Multi-valued)
- Add User NON-CUA XSL Stylesheets (Multi-valued)

These advanced mappings have been merged into the remaining mapping options for Add. Changes to your custom XSL transforms and add advanced mapping may be required. See “ADD ADVANCED MAPPING TAB” on page 86 for more details.

The following Modify Advanced Mapping options have been removed:

- Modify User CUA XSL Stylesheets (Multi-valued)
- Modify User NON-CUA XSL Stylesheets (Multi-valued)

These advanced mappings have been merged into the remaining mapping options for Modify. Changes to your custom XSL transforms and modify advanced mapping may be required. See “MODIFY ADVANCED MAPPING TAB” on page 86 for more details.

The following Reconciliation Advance Mapping options have been removed:

- Search User CUA Roles Request Lookup XSL Stylesheet
- Search User CUA Roles Response Lookup XSL Stylesheet
- Search User CUA Profiles Request Lookup XSL Stylesheet
- Search User CUA Profile Response Lookup XSL Stylesheet

These advanced mappings have been merged into the remaining mapping options for reconciliations. Changes to your custom XSL transforms and reconciliation advanced mapping may be required. See “RECONCILIATION ADVANCED MAPPING TAB” on page 87 for more details.

SAP JCo upgrade

From version 6.0.8, the SAP NetWeaver Adapter only supports JCo version 3.0.9.

You must download the 3.0.9 version of the JCo for upgrading.

If you plan to deploy the adapter on a Windows platform, Microsoft Visual C++ 2005 libraries are also required. See the Microsoft Knowledge Base article 973544 for instructions on obtaining and installing the required Microsoft Visual C++ 2005 libraries.

Chapter 5. Configuring

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

See the *IBM Security Dispatcher Installation and Configuration Guide* for 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 SAP NetWeaver Adapter JAR file. You might customize the adapter profile to change the account form or the service form. 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.

About this task

The JAR file is included in the SAP NetWeaver Adapter compressed file that you downloaded from the IBM website.

The following files are included in the SAP NetWeaver JAR file:

- CustomLabels.properties
- ersapnwaccount.xml
- ersapnwservice.xml
- SapNWAssemblyLines.xml
- schema.dsml
- service.def

Procedure

1. To edit the JAR file, log on to the workstation where the SAP NetWeaver Adapter is installed.
2. Copy the JAR file into a temporary directory.
3. Extract the contents of the JAR file into the temporary directory.

   The following example applies to the SAP NetWeaver Adapter profile. Type the name of the JAR file for your operating system. Run the following command.

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

   The **`jar`** command extracts the files into the `SAPNWProfile` 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

   Run the following commands:

```
#cd /tmp
#jar -cvf SapNWProfile.jar SAPNWProfile
```

6. Import the JAR file into the IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager application server.
7. Stop and start the Identity server.
8. Restart the adapter service.

XSL style sheets

The adapter can be configured by modifying the XSL style sheet advanced mappings.

Before the adapter runs an SAP RFC, it queries the CUA status of the target SAP system. If the CUA status is `true`, then the adapter runs the CUA XSL transformations that are in the following lists. If the SAP system is NON-CUA, status `false`, then the adapter runs the NON-CUA XSL transformations. These transformations are in the following lists.

Note: In some cases the default XSL transformations are the same for both CUA and NON-CUA systems.

The adapter functions without requiring any advanced mapping XSL transformations to be configured. The default values for each advanced mapping in the following lists are used. However, any advanced mappings that are configured by the user, override the listed default XSL transformations.

ADD ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing add operation requests.

Add User Basic XSL Stylesheets

This attribute is a multi-valued attribute where each value is separated by a single space (‘ ‘) character. The values are file names that represent the order in which the adapter runs XSL transformations on the user account data. The data is sent from IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager during an **add** operation request. The XSL results are run as RFC calls against the target SAP system.

The values are the names of the XSL files that are deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

CUA:

```
xsl/sapnw_bapi_user_create.xsl
xsl/sapnw_bapi_user_disablepassword.xsl
xsl/sapnw_bapi_user_system_assign.xsl
xsl/sapnw_bapi_user_change_licensedata.xsl
xsl/sapnw_bapi_user_locactgroups_assign.xsl
xsl/sapnw_bapi_user_locprofiles_assign.xsl
```

NON-CUA:

```
xsl/sapnw_bapi_user_create.xsl
xsl/sapnw_bapi_user_disablepassword.xsl
xsl/sapnw_bapi_user_change_licensedata.xsl
xsl/sapnw_bapi_user_actgroups_assign.xsl
xsl/sapnw_bapi_user_profiles_assign.xsl
```

MODIFY ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing **modify** operation requests.

Modify User Basic XSL Stylesheets

This attribute is a multi-valued attribute where each value is separated by a single space (‘ ‘) character. The values are file names that represent the order in which the adapter runs XSL transformations on the user account data. The data is sent from IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager during a **modify** operation request. The XSL results are run as RFC calls against the target SAP system.

The values are the names of XSL files that are deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

CUA:

```
xsl/sapnw_bapi_user_change.xsl
xsl/sapnw_bapi_user_disablepassword.xsl
xsl/sapnw_bapi_user_system_assign.xsl
xsl/sapnw_bapi_user_change_licensedata.xsl
xsl/sapnw_bapi_user_locactgroups_assign.xsl
xsl/sapnw_bapi_user_locprofiles_assign.xsl
```

NON-CUA:

```
xsl/sapnw_bapi_user_change.xsl
xsl/sapnw_bapi_user_disablepassword.xsl
xsl/sapnw_bapi_user_change_licensedata.xsl
xsl/sapnw_bapi_user_actgroups_assign.xsl
xsl/sapnw_bapi_user_profiles_assign.xsl
```

Modify User Basic Lookup Request Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that produces an RFC request. The RFC request is run by the adapter to determine whether the account to be modified is present. If a value is supplied, the transformation is run regardless of the CUA status of the target SAP system. If CUA is used, the following XSL mappings are required:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl xsl/
sapnw_bapi_user_locactgroups_read_precall.xsl
```

The value is the name of the XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl
```

Modify User Basic Lookup Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that will process the SAP response from running the RFC call that is based on the setting of **Modify User Lookup Request Stylesheet**. If a value is supplied, the transformation is run regardless of the CUA status of the target SAP system. If CUA is used, the following additional XSL mappings are required:

```
xsl/sapnw_bapi_user_getdetail_postcall.xsl xsl/
sapnw_bapi_user_locactgroups_read_postcall.xsl
```

The value is the name of XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_postcall.xsl
```

DELETE ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing delete operation requests.

Delete User Basic XSL Stylesheets

This attribute is a multi-valued attribute where each value is separated by a single space (‘ ‘) character. The values are file names that represent the order in which the adapter runs XSL transformations on the user account data. The data is sent from IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager during a **delete** operation request. The XSL results are run as RFC calls against the target SAP system. If a value is supplied, the transformations are run regardless of the CUA status of target SAP system.

The values are the names of XSL files that are deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

```
xsl/sapnw_bapi_user_delete.xsl
```

Delete User Basic Lookup Request Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that produces an RFC request. The RFC request is run by the adapter to determine whether the account to be deleted is present. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl
```

Delete User Basic Lookup Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that processes the SAP response from the RFC call. The call is run based on the setting of **Delete User Lookup Request Stylesheet**. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_postcall.xsl
```

SUSPEND ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing suspend operation requests.

Suspend User Basic XSL Stylesheets

This attribute is a multi-valued attribute where each value is separated by a single space (‘ ‘) character. The values are file names that represent the order in which the adapter runs XSL transformations on the user account data. The data is sent from IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager during a **suspend** operation request. The XSL results are run as RFC calls against the target SAP system. If a value is supplied, the transformations are run regardless of the CUA status of target SAP system.

The values are the names of XSL files that are deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

```
xsl/sapnw_bapi_user_lock.xsl
```

Suspend User Basic Lookup Request Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that produces an RFC request. The RFC request is run by the adapter to determine whether the account to be suspended is present. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl
```

Suspend User Basic Lookup Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that processes the SAP response from the RFC call. The call is run based on the setting of **Suspend User Lookup Request Stylesheet**. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_postcall.xsl
```

RESTORE ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing restore operation requests.

Restore User Basic XSL Stylesheets

This attribute is a multivalued attribute where each value is separated by a single space (‘ ‘) character. The values are file names that represent the order in which the adapter runs XSL transformations on the user account data. The data is sent from IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager during a **restore** operation request. The XSL results are run as RFC calls against the target SAP system. If a value is supplied, the transformations are run regardless of the CUA status of target SAP system.

The values are the names of XSL files that are deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

```
xsl/sapnw_bapi_user_unlock.xsl
```

Restore User Basic Lookup Request Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that produces an RFC request. The RFC request is run by the adapter to determine whether the account to be restored is present. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl
```

Restore User Basic Lookup Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that processes the SAP response from the RFC call. The call is run based on the setting of **Restore User Basic Lookup Request Stylesheet**. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of the XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_postcall.xsl
```

CHANGE PASSWORD ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing password operation requests.

Change Password Basic XSL Stylesheets

This attribute is a multi-valued attribute where each value is separated by a single space (‘ ‘) character. The values are file names that represent the order in which the adapter runs XSL transformations on the user account data. The data is sent from IBM Security Verify IdentityIBM

Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager during a **password** operation request. The XSL results are run as RFC calls against the target SAP system. If a value is supplied, the transformations are run regardless of the CUA status of target SAP system.

The values are the names of XSL files that are deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

```
xsl/sapnw_bapi_user_change.xsl
```

Change Password Basic Lookup Request Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that produces an RFC request. The RFC request is run by the adapter to determine whether the account to be modified is present. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of the XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl
```

Change Password Basic Lookup Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that processes the SAP response from the RFC call. The call is run based on the setting of **Change Password Basic Lookup Request Stylesheet**. If a value is supplied, the transformation is run regardless of the CUA status of target SAP system.

The value is the name of the XSL file that is deployed with the adapter relative to the Dispatcher solution directory. If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_postcall.xsl
```

RECONCILIATION ADVANCED MAPPING TAB

Settings of this tab apply only when the adapter is processing reconciliation and search operation requests.

Search User Basic Select Request XSL Stylesheets

This attribute is a multi-valued attribute. The value is a list of XSL transformation file names that are separated by space (" "). Each transform is run in the defined order and produce an RFC request. Each RFC request is run by the adapter. If more than one transform and resulting RFC is run, the result of each RFC call is appended to an XML result document with a root tag named `<bapiResults>`. This result list is passed to the **Search User Basic Select Response XSL Stylesheets**. If only one XSL file name is supplied, the resulting RFC is run, and its response will be passed directly to **Search User Basic Select Response XSL Stylesheets**.

Each XSL transform file must be deployed with the adapter in the `xsl` directory relative to the Dispatcher solution directory.

If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

```
xsl/sapnw_bapi_user_getlist_precall.xsl
```

Search User Basic Select Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that processes the SAP response or responses from the RFC calls. The calls are run based on the setting of **Search User Basic Select Request Stylesheet**. This transform produces the list of user names to be iterated during the reconciliation.

The XSL transform file must be deployed with the adapter in the `xsl` directory relative to the Dispatcher solution directory.

If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getlist_postcall.xsl
```

Search User Basic Iterate Request XSL Stylesheets

This attribute is a multi-valued attribute. The value is a list of XSL transformation file names that are separated by space (" "). Each transform is run in the defined order and produce an RFC request. Each RFC request is run by the adapter. Each RFC that is run is responsible for returning parts of the user account details. If more than one transform and resulting RFC is run, the result of each RFC call is appended to an XML result document with a root tag named `<bapiResults>`. This result list is passed to the **Search User Basic Iterate Response XSL Stylesheets**. If only one XSL file name is supplied, the resulting RFC is run. The response is passed directly to **Search User Basic Select Response XSL Stylesheets**.

Each XSL transform file must be deployed with the adapter in the `xsl` directory relative to the Dispatcher solution directory.

If no value is supplied, the adapter runs the following XSL transformations and resulting RFC calls:

CUA:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl
xsl/sapnw_bapi_user_locactgroups_read_precall.xsl
xsl/sapnw_bapi_user_locprofiles_read_precall.xsl
```

RFC

NON-CUA:

```
xsl/sapnw_bapi_user_getdetail_precall.xsl
```

Search User Basic Iterate Response Stylesheet

This attribute is a single-valued attribute. The value is the file name of an XSL transformation that processes the SAP response or responses from the RFC calls. The calls are run based on the setting of **Search User Basic Iterate Request Stylesheet**. The result of running this transform is sent to the Identity server.

The XSL transform file must be deployed with the adapter in the `xsl` directory relative to the Dispatcher solution directory.

If no value is supplied, the adapter runs the following XSL transformation and resulting RFC call:

```
xsl/sapnw_bapi_user_getdetail_postcall.xsl
```

SAP Attribute PARAMETER is limited to 18 characters

According to SAP, the data structure of the BAPI is limited to 18 characters for each parameter value. SAP increased the length of the values to 40 characters and extended the BAPI by adding another data table. By default, the adapter supports PARAMETER. However PARAMETER1 can be incorporated into the adapter by making XSL modifications. For more information on how to use the ITIM Adapter for SAP NetWeaver to manage the 'PARAMETER1' attribute, see Using ITIM Adapter for SAP NetWeaver to Manager 'PARAMETER1' attribute.

BAPI method execution with stateful connection

The SAP JCo 3.x connection between SAP R3 and ISIM, by default, is not stateful. The stateful connection is also required in case of transactional BAPIs. To make the connection stateful between Business Application Programming Interfaces (BAPIs) method execution, add the following tags to the XSL files according to your requirement.

To begin a stateful connection, add this tag to your XSL:

```
<CONTEXT_BEGIN> & </CONTEXT_BEGIN> or <CONTEXT_BEGIN/>
```

To end a stateful connection, add this tag to your XSL:

```
<CONTEXT_END> & </CONTEXT_END> or <CONTEXT_END/>
```

It is not necessary to have both <CONTEXT_BEGIN/> and <CONTEXT_END/> tags in the same XSL. Nested <CONTEXT_BEGIN/> and <CONTEXT_END/> tags can also be implemented, provided that the tags are nested correctly, else unexpected result can occur. Stateful connection started by each <CONTEXT_BEGIN/> tag gets ended by its associated <CONTEXT_END/> tag.

Note: Stateful connection that is started by each <CONTEXT_BEGIN/> tag gets ended by its associated <CONTEXT_END/> tag. If the <CONTEXT_BEGIN/> tag does not have its associated <CONTEXT_END/> tag, the stateful connection gets terminated at the end of JCo connection.

For example, the <CONTEXT_BEGIN/> and <CONTEXT_END/> tags are added to the following files:

- sapnw_bapi_charact_create.xsl file

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
   version="1.0"
   xmlns:xalan="http://xml.apache.org/xslt">
…..
…..
<BAPI_CHARACT_CREATE>
<CONTEXT_BEGIN/>
…..
…..
</BAPI_CHARACT_CREATE>
…..
…..
</xsl:stylesheet>
```

- sapnw_bapi_transaction_commit.xsl file

```
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
   version="1.0"
   xmlns:xalan="http://xml.apache.org/xslt">
…..
…..
<BAPI_TRANSACTION_COMMIT>
…..
…..
<CONTEXT_BEGIN/>
</BAPI_TRANSACTION_COMMIT>
…..
…..
</xsl:stylesheet>
```

Customizing the SAP NetWeaver Adapter

You can customize the adapter to suit your needs.

About this task

You can increase the range of years on IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager for the "Valid From" and "Valid To" calendar widget.

Procedure

1. Use your preferred LDAP browser to locate the following entry:
   erformname=erITIMService,ou=formTemplates,ou=itim,<tenant>,<rootsuffix>
2. Find the **erXML** attribute in the entry.
3. Update the **erXML** attribute to have the following **formElement**:

Set the MIN_YEAR and MAX_YEAR to the year range you want the calendar to display (e.g. from 1900 to 2099). Use the **spanYearRange** option to show the year values between *MIN_YEAR* and *MAX_YEAR*.

```
<formElement direction="inherit" label="$ersapnwdatefrom"
name="data.ersapnwdatefrom">
<dateInput mixYear="MIN_YEAR" maxYear="MAX_YEAR"
spanYearRange="Yes" hoursAndMinutes="false"/>
</formElement>

<formElement direction="inherit" label="$ersapnwdateuntil"
name="data.ersapnwdateuntil">
<dateInput mixYear="MIN_YEAR" maxYear="MAX_YEAR"
spanYearRange="Yes" hoursAndMinutes="false"/>
</formElement>
```

For instance, the following example will have the calendar widget contains all the values from 1900 to 2099.

```
<formElement direction="inherit" label="$ersapnwdatefrom"
name="data.ersapnwdatefrom">
<dateInput mixYear="1900" maxYear="2099" spanYearRange="Yes"
hoursAndMinutes="false"/>
</formElement>
```

Note:

- It is NOT recommended to combine **spanYearRange** and a **maxYear** of 9999. Because this will significantly increase the amount of data that must be sent to the browser for the page to be displayed, and will hurt performance.
- If you want to include years earlier than 1990, then use the **minYear** attribute. For example, `<dateInput minYear="1974"/>`.
- Any customization done through the IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager UI (Form Editor Applet) MUST be done prior to adding any manual date attribute modifications. The Form Editor UI is not equipped to handle these additional date attribute customizations. When edited, the Form Editor UI will write out standard Date attributes regardless of any manual modification previously added. Thus, the manual updates must be redone, or their functionality will be not be effective.

4. Save the updated **erXML** attribute to the LDAP.

Support for SAP productive passwords

SAP provides support for the use of productive passwords with the standard Business Application Programming Interface (BAPI). A productive password is a single password that can be used on heterogeneous SAP systems.

To allow the SAP NetWeaver Adapter to set productive passwords:

- SAP NetWeaver AS ABAP uses SAP Cryptographic Library as its security provider for Secure Network Communication (SNC).
- SAP NetWeaver AS ABAP is configured to use Secure Network Communication for RFC communications.
- The SAP user account that is used by the adapter to communicate with SAP NetWeaver AS ABAP has the authorization for object **S_USER_GRP** with activity **PP**.
- The adapter is configured to use Secure Network Communication for its communication with SAP NetWeaver AS ABAP.

Refer to SAP note 1287410. You must have S-user credentials that are provided by SAP to access this website.

Configuring Secure Network Communication between the adapter and SAP NetWeaver AS ABAP

Use Secure Network Communication (SNC) to secure the communication between the adapter and SAP NetWeaver AS ABAP.

Complete the following tasks:

- "Installing the SAP Cryptographic Library" on page 108
- "Creating a Person Security Environment for the adapter" on page 109
- "Importing the public certificate of the adapter into the SAP NetWeaver AS ABAP Person Security Environment" on page 110
- "Importing the SAP NetWeaver AS ABAP public certificate into the Person Security Environment of the adapter" on page 111
- "Allowing the user account of the adapter to connect to SAP NetWeaver AS ABAP by using Secure Network Communication" on page 112
- "Setting optional RFC connection parameters for the adapter" on page 112
- "Verifying the Secure Network Communication setup" on page 113

These configuration tasks have been verified against the following SAP versions:

Table 8. SAP version support

SAP release and version	Software component	Support package
700	SAP_BASIS	SAPKB70019
701	SAP_BASIS	SAPKB70111
702	SAP_BASIS	SAPKB70210
710	SAP_BASIS	SAPKB71010
730	SAP_BASIS	SAPKB73000
731	SAP_BASIS	SAPKB73102

For information on required configuration changes to subsequent versions, review the SAP documentation for Secure Network Communication, SAP Cryptographic Library, and productive password support at http://help.sap.com.

Installing the SAP Cryptographic Library

You can use these steps to install the SAP Cryptographic Library.

Procedure

1. Download the SAP Cryptographic Library from the SAP Service Marketplace and extract it to a temporary directory.
2. Copy the library and the command line tool to a local directory on the system that hosts the adapter. For example:

   Windows systems

   ```
   C:\usr\sap\sapcrypto.dll
   C:\usr\sap\sapgenpse.exe
   ```

   UNIX systems

   ```
   /usr/sap/libsapcrypto.so
   /usr/sap/sapgenpse
   ```

3. Copy the license ticket (ticket) to a subdirectory that is named `sec`.
   For example:

   Windows systems

   ```
   C:\usr\sap\sec\ticket
   ```

   UNIX systems

   ```
   /usr/sap/sec/ticket
   ```

4. For the user that runs the adapter, set the environment variable **SECUDIR** to this directory.
   For example:

   Windows systems

   ```
   SECUDIR=C:\usr\sap\sec
   ```

   UNIX systems

   ```
   SECUDIR=/usr/sap/sec
   ```

   If the user is the SYSTEM user, set **SECUDIR** as a system variable.
5. Restart the adapter (RMI dispatcher service) so that the new environment variable is accessible by the adapter.

Creating a Person Security Environment for the adapter

You can use these steps to create a Person Security Environment for the adapter.

Procedure

1. Start a command line console and change to the directory that contains the **sapgenpse** tool.
2. Create a Person Security Environment for the adapter.
   Running this command:

   ```
   sapgenpse get_pse [-p PSE_name] [-x PIN] [DN]
   ```

   Where:

   -p *PSE_name*
   Path and file name for Person Security Environment for the adapter.

   -x *PIN*
   PIN value that protects the Person Security Environment.

   DN
   Distinguished Name for the adapter. The Distinguished Name is used to build the Secure Network Communication name for the adapter. The Distinguished Name has the following elements:

   - CN = *Common_Name*
   - OU = *Organizational_Unit*
   - O = *Organization*
   - C = *Country*

   For example:

   ```
   sapgenpse get_pse -p adapter.pse -x passw0rd "CN=adapter,OU=IdM,O=IBM,C=US"
   ```

3. Use the following command (on one line) to open the adapter's Person Security Environment and create credentials:

   ```
   sapgenpse seclogin [-p PSE_name] [-x PIN] [-O [NT_Domain\]user_ID]
   ```

Where:

-p *PSE_name*
Path and file name for the Person Security Environment for the adapter.

-x *PIN*
PIN value that protects the Person Security Environment.

-O [*NT_Domain*\[*user_ID**
User for whom the credentials are created. Specify the user that runs the adapter service. Omitting this value specifies the current user.

For example:

```
sapgenpse seclogin -p adapter.pse -x passw0rd -O SYSTEM
```

Importing the public certificate of the adapter into the SAP NetWeaver AS ABAP Person Security Environment

You can use these steps to import the public certificate of the adapter into the SAP NetWeaver AS ABAP Person Security Environment.

Procedure

1. Export the public certificate of the adapter.
   Run the following command:

   ```
   sapgenpse export_own_cert [-o output_file] [-p PSE_name] [-x PIN] [DN]
   ```

   Where:

   -o *output_file*
   Path and file name for the exported certificate.

   -p *PSE_name*
   Path and file name for Person Security Environment for the adapter.

   -x *PIN*
   PIN value that protects the Person Security Environment.

   For example:

   ```
   sapgenpse export_own_cert -o adapter.crt -p adapter.pse -x passw0rd
   ```

2. Start Trust Manager from SAP graphical user interface (transaction STRUST).
3. Select (double-click) the SAP Person Security Environment under the SAP`Cryptolib` folder.
4. When prompted, enter the PIN value.
5. Select **Certificate > Import** from the menu.
6. Enter the path and file name of the public certificate of the adapter.
7. Select the Base64 format and choose Enter.
   The certificate appears in the **Certificate** section of **Trust Manager** panel.
8. Click **Add to Certificate List** button to add the certificate to the Person Security Environment.
9. Save the data.

   Note: For securing multiple SAP systems with a single Secure Network Communication certificate, repeat steps 2 - 9 for each SAP system. Use the same certificate from step 1 to upload to different SAP systems.

Importing the SAP NetWeaver AS ABAP public certificate into the Person Security Environment of the adapter

You can use these steps to import the SAP NetWeaver AS ABAP public certificate into the Person Security Environment of the adapter.

Procedure

1. In Trust Manager, select the SAP NetWeaver AS ABAP Secure Network Communication Person Security Environment.
2. Select (double-click) the certificate in the **Owner** field.
3. Select **Certificate -> Export** from the menu.
4. Specify the path and file name to save the file; select the Base64 format and choose Enter.

   Use a different file name for each SAP system.
5. Copy the exported certificate to the system that hosts the adapter.
6. On the adapter system, run the following command on one line to import the SAP NetWeaver AS ABAP public certificate into the Person Security Environment of the adapter:

   ```
   sapgenpse maintain_pk [-a cert_file] [-p PSE_name] [-x PIN] [DN]
   ```

   Where:

   -a *cert_file*
   Path and file name for the SAP NetWeaver AS ABAP public certificate.

   -p *PSE_name*
   Path and file name for Person Security Environment for the adapter.

   -x *PIN*
   PIN value that protects the Person Security Environment.

   For example:

   ```
   sapgenpse maintain_pk -a sap.crt -p adapter.pse
   ```
7. Run the following command to display all the certificate details that were updated in the `.pse` file.

   ```
   sapgenpse maintain_pk -l -p PSE_name [-x PIN]
   ```

   Where:

   -p *PSE_name*
   Path and file name for Person Security Environment for the adapter.

   -x *PIN*
   PIN value that protects the Person Security Environment.

   For example:

   ```
   sapgenpse maintain_pk -l -p adapter.pse
   ```

   Note: For securing multiple SAP systems with a single Secure Network Communication certificate, repeat steps 1 to 6 for each SAP system. To update the file entry of the certificates that were exported from different SAP systems to the existing `.pse` file, run step 6 for each of the certificates.

Allowing the user account of the adapter to connect to SAP NetWeaver AS ABAP by using Secure Network Communication

You can allow the user account of the adapter to connect to SAP NetWeaver AS ABAP.

Procedure

1. In the SAP graphical user interface, start **Table Maintenance** (transaction SM30).
2. Maintain the table **USRACLEXT**.
3. Select **New Entries**.
4. Enter the following data in the corresponding fields:

   User
   Specify the user that the adapter uses to connect to SAP NetWeaver AS ABAP.

   Sequence Number
   Enter `000` unless the user has more than one Secure Network Communication name.

   SNC Name
   Specify the DN that is associated with the Person Security Environment of the adapter. For example:

   ```
   p: CN=adapter,OU=IdM,O=IBM,C=US
   ```

5. Save the data.

   Note: For securing multiple SAP systems with a single Secure Network Communication certificate, repeat steps 1 - 5 for each SAP system.

Setting optional RFC connection parameters for the adapter

To enable the adapter to use Secure Network Communication to communicate with SAP NetWeaver AS ABAP, you must add parameters to the service form.

Procedure

Add these parameters on one line to the **Optional RFC Connection Parameters** field in the service form:

```
snc_mode=1|snc_partnername=as_abap_snc_name|
snc_qop=3|snc_myname=adapter_snc_name|snc_lib=path_to_snc_lib
```

Where:

snc_mode
Secure Network Communication activation indicator. Use these values:

0
Secure Network Communication is disabled.

1
Secure Network Communication is activated.

snc_partnername
Secure Network Communication name of the communication partner (SAP NetWeaver AS ABAP).

snc_qop
Quality of protection level.

1
Secure authentication only.

2
Data integrity protection.

3
Data privacy protection.

9
Use the value from `snc/data_protection/max`.

snc_myname
Secure Network Communication name of the adapter.

For example (on one line):

```
snc_mode=1|snc_partnername=p:CN=GC8,OU=IdM,O=IBM,C=US|snc_qop=3|
snc_myname=p:CN=adapter,OU=IdM,O=IBM,C=US|snc_lib=C:/usr/sap/sapcrypto.dll
```

Note: For securing multiple SAP systems with single Secure Network Communication certificate, pass same path value for `snc_lib` in the service forms of all the SAP systems.

Note: These parameters directly correspond to SAP JCO properties for Secure Network Communication except that they do not have the **`jco.client.`** prefix. The adapter automatically prepends the string **`jco.client.`** before the adapter passes these parameters to SAP JCO.

For more information about the Secure Network Communication parameters, see the SAP Help Portal.

Verifying the Secure Network Communication setup

Verify if you have a proper setup of the Secure Network Communication to ensure secure communication between the adapter and SAP NetWeaver AS ABAP and to avoid possible configuration issues.

Procedure

1. Make sure the following files are in their corresponding folders in the client system, where the IBM Security Directory Integrator is running.

Folder	Files
\usr\sap	• `sapcrypto.dll` • `sapgenpse.exe` • local certificate • server certificate
\usr\sap\sec	• `adapter.pse` • cred_v2 • ticket

2. Make sure all the files used from the SAP cryptolibrary packages are unused.
3. Make sure the `sapcrypto.dll` file is a Win32 file. Otherwise, you are prompted that the `sapcrypto.dll` file is not a valid Win32 application.
4. Use the following command to check the certificate entry in the `sapgenpse` file:

   ```
   sapgenpse maintain_pk -l -p <PSE_name> [-x <PIN>]
   ```

   Where:

   -l
   Returns the list of existing certificates.

   -p <PSE_name>
   Specifies the path and file name for the server's PSE.

   -x <PIN>
   Specifies the PIN that protects the PSE
5. Make sure the entry to USRACLEXT (table) in SM30 (t-code) complies with the following requirements:

- Starts with "p"
- Contains the details of the local certificate
- Does not have any space after a period "."
- Includes the canonical name

6. The server certificate name must be selected in STRUST (t-code) when you download it.
7. Make sure each parameter in the Optional RFC parameter complies with the following requirements:
   - Separated using a pipe "|"
   - Does not have any space after a period "."

Configuring the adapter to send only the role name to SAP

See this topic if you want to send only the role names.

About this task

SAP sets the default start and end date for the role. The start date is the current date and the end date is 12-31-9999.

Procedure

1. Import the `SapNWProfile.jar` file on IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager.
2. From the Design form, modify the account attribute `ersapnwagrname` to List box. Specify the following values.

Table 9. Attributes and values

Attribute	Value
searchbase	context
attribute	erSAPagrname
source attribute	erSAPagrname
objectclass	erSAProleList
filter	(objectclass=erSAProleList)

3. Specify the XSL file names.

   Note: Do not change the sequence of the XSL files.

Table 10. XSL file names for a non-CUA system

Table Name	Label Name	XSL
Reconciliation Advanced Mapping	Search User Basic Iterate Response XSL Stylesheet (Single-valued)	• `xsl/sapnw_bapi_user_getdetail_postcall_role_only.xsl`
Add Advanced Mapping	Add User Basic XSL Stylesheets (Multi-valued)	• `xsl/sapnw_bapi_user_create.xsl` • `xsl/sapnw_bapi_user_disablepassword.xsl` • `xsl/sapnw_bapi_user_system_assign.xsl` • `xsl/sapnw_bapi_user_change_licensedata.xsl` • `xsl/sapnw_bapi_noncua_r_only_assign.xsl` • `xsl/sapnw_bapi_user_profiles_assign.xsl`

Table 10. XSL file names for a non-CUA system (continued)

Table Name	Label Name	XSL
Modify Advanced Mapping	Modify User Basic XSL Stylesheets (Multi-valued)	• xsl/sapnw_bapi_user_change.xsl • xsl/sapnw_bapi_user_disablepassword.xsl • xsl/sapnw_bapi_user_system_assign.xsl • xsl/sapnw_bapi_user_change_licensedata.xsl • xsl/sapnw_bapi_noncua_r_only_assign.xsl • xsl/sapnw_bapi_user_profiles_assign.xsl
	Modify User Basic Lookup Response XSL Stylesheet (Single-valued)	• xsl/sapnw_bapi_user_getdetail_postcall_role_only.xsl

Table 11. XSL file names for a CUA system

Tabe Name	Label Name	XSL
Reconciliation Advanced Mapping	Search User Basic Iterate Response XSL Stylesheet (Single-valued)	• xsl/sapnw_bapi_user_getdetail_postcall_role_only.xsl
Add Advanced Mapping	Add User Basic XSL Stylesheets (Multi-valued)	• xsl/sapnw_bapi_user_create.xsl • xsl/sapnw_bapi_user_disablepassword.xsl • xsl/sapnw_bapi_user_system_assign.xsl • xsl/sapnw_bapi_user_change_licensedata.xsl • xsl/sapnw_bapi_cua_r_only_assign.xsl • xsl/sapnw_bapi_user_locprofiles_assign.xsl
Modify Advanced Mapping	Modify User Basic XSL Stylesheets (Multi-valued)	• xsl/sapnw_bapi_user_change.xsl • xsl/sapnw_bapi_user_disablepassword.xsl • xsl/sapnw_bapi_user_system_assign.xsl • xsl/sapnw_bapi_user_change_licensedata.xsl • xsl/sapnw_bapi_cua_r_only_assign.xsl • xsl/sapnw_bapi_user_locprofiles_assign.xsl
	Modify User Basic Lookup Response XSL Stylesheet (Single-valued)	• xsl/sapnw_bapi_user_getdetail_postcall_role_only.xsl

Chapter 6. Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Logs

Logs added to the log file for the adapter or the Dispatcher have a specific format.

```
<Log Level> [<Assembly Line_ProfileName>_<Request Id>]_
[<Connector Name>] - <message>
```

Log Level
Specifies the logging level that you configured for the adapter. The options are DEBUG, ERROR, INFO, and WARN. For information about using the `log4j.properties` file to configure logging, see the *Dispatcher Installation and Configuration Guide*.

Assembly Line
Specifies the name of the assembly line that is logging the information.

ProfileName
Specifies the name of the profile. Profile names may vary based on the adapter that is running or the operating system.

Request ID
Specifies the number of the request. The Request ID is used to uniquely identify a specific request.

Connector Name
Specifies the adapter connector.

Message
Specifies the informational message .

When the **Test** button on the SAP NetWeaver Adapter service form is clicked, service, environment and configuration values are sent to the IBM Security Directory Integrator log during the test. The information collected during the test may assist in diagnosing issues.

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.

This table describes the error messages displayed during run time and corresponding problem descriptions.

Table 12. Error messages and problem descriptions

Error messages	Problem descriptions
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGIMT401E An error occurred while starting the AssemblyLines/SapNWTest_SAP - TV2_test-no-requestid_9dbf1884-29b1-11b2-689a-00000a020011 agent. Error: java.lang.ExceptionInInitializerError: Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: sapjco3 (Not found in java.library.path) operation on the IBM Security Directory Integrator server. Error: {1}	Microsoft Visual C++ 2005 libraries are not installed, or permissions for .dll file are not correct. Verify installation steps and permissions.
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGDIS067E Unable to find configuration for AssemblyLine SapNWTest_SAP_R/3_NW_test-no-requestid_c41b1d60-28f8-11b2-e832-00001ff87342.]	The service name might contain special characters that IBM Security Directory Integrator can not handle, for example “/”.
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGDIS809E handleException - cannot handle exception , script java.lang.NoClassDefFoundError: com.sap.conn.jco.ext.DestinationDataProvider	SAP JCo is not installed, or permissions for .jar file are not correct. Verify installation steps and permissions.

Table 12. Error messages and problem descriptions (continued)

Error messages	Problem descriptions
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** Caused by: java.io.FileNotFoundException: app/itdi611/solution/xsl/ sapnw_bapi_errors.properties (No such file or directory)	Property and .xsl files are copied to the wrong directory during the adapter installation, or file permissions are not correct. Verify installation steps and permissions.
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGDIS809E handleException - cannot handle exception , script java.lang.ExceptionInInitializerError: Error getting the version of the native layer: java.lang.UnsatisfiedLinkError: sapjco3 (Not found in java.library.path)	Path for SAP JCo dynamic library is not correct. Correct it and restart the adapter service.
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** Exception Class:org.xml.sax. SAXParseExceptionorg.xml.sax. SAXParseException: Invalid byte 1 of 1-byte UTF-8 sequence.	Java property "–`Dfile.encoding=UTF-8`" needs to be added. Add the property as described in the Installation Guide and Release Notes, and restart the adapter service.

Table 12. Error messages and problem descriptions (continued)	
Error messages	**Problem descriptions**
Reconciliation doesn't return all SAP accounts. Reconciliation is successful but some accounts are missing.	For the adapter to reconcile a large number of accounts successfully, you might need to increase Websphere's JVM memory. To do so, complete the following steps on the WebSphere host machine: **Note:** The JVM memory should not be increased to a value higher than the System memory. 1. Login to the WebSphere Administrative Console. 2. From the left menu, select **Servers** and then **Application Servers**. 3. A table displays the names of known application servers on your system. Click the link for your primary application server. 4. On the **Configuration** tab, select **Process Definition**. 5. Select the **Java Virtual Machine** property. 6. Enter a new value for **Maximum Heap Size**. The default value is 256 MB. If the allocated JVM memory is not large enough, an attempt to reconcile a large number of accounts using the IBM Security Access Manager Adapter will result in log file errors, and the reconciliation process will not complete successfully. The Adapter log files will contain entries stating ErmPduAddEntry failed. The `WebSphere_install_dir/logs/itim.log` file will contain **java.lang.OutOfMemoryError** exceptions.

Reconciliation of supporting data

All supporting data can be reconciled through the use of the search filter in the reconciliation query.

To reconcile supporting data only, use the following search filter:

```
(!(objectclass=ersapnwaccount))
```

The SAP systems can have tens of thousands of roles, profiles, and other support data entries. To reconcile accounts only, use the following search filter:

```
(objectclass=ersapnwaccount)
```

Improving reconciliation operation performance

Use Java settings to improve the performance of reconciliation operation.

Procedure

1. Navigate to the *JAVA_Home*/lib directory.
2. Rename jaxp.properties.sample to jaxp.properties.
3. In the jaxp.properties file, remove the comment tags for the following properties:

```
javax.xml.transform.TransformerFactory=
  com.ibm.xtq.xslt.jaxp.compiler.TransformerFactoryImpl
javax.xml.xpath.XPathFactory=
  org.apache.xpath.jaxp.XPathFactoryImpl
javax.xml.parsers.SAXParserFactory=
  org.apache.xerces.jaxp.SAXParserFactoryImpl
javax.xml.parsers.DocumentBuilderFactory=
  org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
```

4. Check the performance of reconciliation operation. If it fails, continue to step 5.
5. Set the following system property:

```
export IBM_JAVA_OPTIONS=-Djavax.xml.transform.TransformerFactory=
  org.apache.xalan.processor.TransformerFactoryImpl
```

6. Check the performance of reconciliation operation again.

For more information about the earlier settings, see the following resources:

Chapter 7. 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.

Procedure

1. Stop the IBM Security Verify Identity (Dispatcher) Service.
2. Remove the SAP NetWeaver Adapter JAR files.
   a. Delete `SapNWSupport.jar` and and `SapNWUserConnector.jar` from the *`ITDI_HOME`*`/jars/connectors` directory.
   b. Delete `SapNWRfc.jar` from the *`ITDI_HOME`*`/jars/functions` directory.
3. Remove the adapter stylesheets from the `ITDI_HOME/`*`solution`*`/xsl` directory.
4. Delete the adapter profile from the IBM Security Verify Identity server.

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

Chapter 8. Reference

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

Adapter attributes and object classes

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.

After you install the adapter profile, the SAP NetWeaver Adapter supports a standard set of attributes.

The following table lists the standard attributes supported by the SAP NetWeaver Adapter.

Table 13. Supported account attributes

IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Name	**Attribute Name**	**Description**	**Data Type**
Academic title	ersapnwacademic	Dr., Prof., and so on	SAP predefined value
Account	ersapnwldaccount	User account identification	Character or numeric string, which is not SAP predefined
Authorization Profiles	ersapnwprofile	Authorization Profiles	SAP predefined value
Authorization Roles	ersapnwagrname	Role name	Character or numeric string
Building	ersapnwbuilding	Building number	Character or numeric string
CATT Status	ersapnwcatt	CATT test status	Yes or No
Company	ersapnwcompany	Company Name	String
Cost Center	ersapnwcostcenter	User cost center	Character or numeric string
Country	ersapnwcountry	Country key code of user	Character or numeric string, SAP country key
Date Format	ersapnwdateformat	Date format	SAP predefined value, 5 date format versions

Table 13. Supported account attributes (continued)

IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Name	Attribute Name	Description	Data Type
Decimal Notation	ersapnwdecimalpoint	Decimal notation, either period or comma	Character or numeric string
Delete After Print	ersapnwprntdelete	Delete after print	Character or numeric string
Department	ersapnwdepartment	Department	Character or numeric string
Email Address	ersapnwemailaddress	A user can have more than one email address. Refer to the E-mail section under “Special attributes” on page 128 for more information.	Character or numeric string
Fax Number	ersapnwprimaryfaxnumber	Telefax number	Character or numeric string
Fax extension	ersapnwprimaryfaxextension	Fax number: extension	Character or numeric string
Full Name	ersapnwfullname	Full Name See “Special attributes” on page 128 for more details.	String
Function	ersapnwfunction	Function of user	Character or numeric string
Given Name	ersapnwgivenname	First name	Character or numeric string
Group	ersapnwusergroups	User group	SAP predefined value
Insecure Communication Permitted?	ersapnwsncflag	Flag that allows non-secure communiation	SAP Boolean
Internet User Alias	ersapnwalias	Internet user alias	String
Language	ersapnwcommlang	Language set in the user's address record	String

Table 13. Supported account attributes (continued)

IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Name	**Attribute Name**	**Description**	**Data Type**
Last Logged in Date	ersapnwlastlogondate	Last Logged in Date and time of SAP User in ZULU format. For example, YYYYMMDDHHMMZ. This is read-only The date and time is based on the time zone used in the SAP NetWeaver server. This attribute will be supported for SAP NetWeaver 730 and above.	Character or Numeric string, which is not SAP predefined
Logon Language	ersapnwdefaultlang	User's default login language	String
Output Device	ersapnwoutputdevice	Device	SAP predefined value
Password	erpassword	Password to log into SAP system Required for all requests.	SAP predefined value
Personal Time Zone	ersapnwtimezone	Timezone	SAP predefined value, existing timezone remains if a conflict is noted
Print Immediately	ersapnwprntimmediate	Print immediately	Character or numeric string
Room Number	ersapnwroom	Room number	Character or numeric string
Security Policy	ersapnwsecuritypolicyname	Security Policy This attribute is supported for SAP NetWeaver 740 and later.	SAP predefined value
Set Parameter|value	ersapnwparid	Parameter identification	SAP predefined value

Table 13. Supported account attributes (continued)			
IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Name	**Attribute Name**	**Description**	**Data Type**
Set Password as Productive	ersapnwprodpwdflag	This send only flag changes the initial password to productive password. See “Special attributes” on page 128 for more details.	True or False
Start Menu	ersapnwmenu	SAP start menu	SAP predefined value
SNC Name	ersapnwsncname	Printable SNC name	String
Surname	ersapnwsurname	Last name	Input supplied
Telephone Number	ersapnwprimaryphonenumber	Main telephone number	Character or numeric string
Telephone Extension	ersapnwprimaryphoneextension	Telephone number: extension	Character or numeric string
Title	ersapnwtitle	Form of address: Mr., Mrs., Ms	Character or numeric string
User Type	ersapnwtype	User type (A=online, C=CPIC, D=BDC, O=ODC)	SAP predefined value, between 1 and 4, defaults to dialog user
UserName	eruid	User's login ID	String
Valid From	ersapnwdatefrom	Valid from date	Up to 6 data format versions

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.This topic is not applicable for this adapter.

Special attributes

The SAP NetWeaver Adapter supports some special attributes that are specific to the adapter.

Email Address

The SAP email is a multi-valued attribute, which means a user can have more than one email address. You must designate one email address as the user's "Standard" email. In addition, you can designate an email address to be the "Home" email. If only one email address is to be assigned to the account, ensure that you set both the "Standard" email and "Home" email options.

To enter an email address on the IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager form, you must follow this syntax:

```
a|b|c|d
a= X for Standard email, or space for not Standard.
b= is the email address.
c= X for home email, or space for not home.
d= is the sequence number, must consist of three digits.
```

For example, to enter three email addresses for user Jon Doe:

```
X|jon.doe@company.com| |001  (standard email)
 |jon.doe@home.com|X|002     (home email)
 |jon.doe@other.com| |003    (other email)
```

Or, to enter one email address as the standard and home:

```
X|jon.doe@company.com|X|001
```

CUA License Data

To edit license data for CUA systems, the adapter schema supports an attribute named "ersapnwliccuadata". This attribute is a multivalued attribute that enables the management of CUA License Data. This attribute is exposed on the CUA Systems License Data tab. The ersapnwliccuadata attribute consists of nine values that are delimited by pipes and contains no white space. Any data input by the CUA Systems License Data tab overwrites the CUA license data in SAP NetWeaver for the account.

The format of the ersapnwliccuadata attribute is:

```
<CUA System Name>|<ersapnwlicutype>|<ersapnwlicspecver>|<ersapnwlicsurchrg>|
<ersapnwlicsubfrom>|<ersapnwlicsubto>|<ersapnwlicsysid>|<ersapnwlicclient>|
<ersapnwlicbname>|
```

The previous values have the following meanings:

- CUA System Name: CUA Logical system name
- ersapnwlicutype: Contractual User Type
- ersapnwlicspecver: Assignment to special version
- ersapnwlicsurchrg: Country surcharge
- ersapnwlicsubfrom: Substitute date from
- ersapnwlicsubto: Substitute date to
- ersapnwlicsysid: Chargeable user SAP system
- ersapnwlicclient: Chargeable user client
- ersapnwlicbname: Chargeable user name

CUA license data must be input in the CUA Systems License Data tab by using the format that is specified for the ersapnwliccuadata attribute. Some examples of individual entries are:

```
AA1CLNT100|11||0|||AA2|300|HSMITH|
AA5CLNT110|01|91|0||||||
```

Set Password as Productive

This attribute is supported by both **Add** and **Modify** operation. Select this attribute to make the existing password Productive (Permanent). Otherwise, the password is Initial (Temporary). This attribute is available in account form. As such, to select between productive and initial password during the Password

change operation, complete a Modify operation prior to the Password change operation to change the flag.

Note: This is a send only attribute. The value of the flag is not stored in IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager.

Full Name

Pass the full name of the user to this attribute. The full name is reflected in NW against the FORMAT attribute (in SU01) for any string value that is passed except for blank spaces. If the value is blank space or empty, then the FORMAT attribute (in SU01) combines the First name and Last Name that are available in the NW account.

Adapter configuration properties

For guidance on setting IBM Security Directory Integrator configuration properties for the operation of the SAP NetWeaver Adapter, see the *Dispatcher Installation and Configuration Guide*.

Index

T

U

V