IBM Security Verify Governance

# *SAP HR feed adapter Installation and Configuration Guide*

IBM

# Contents

**Figures......................................................................................................v**

**Tables.....................................................................................................vii**

**Chapter 1. Overview.............................................................................1**

Features of the adapter.............................................................................1
Architecture...............................................................................................1
Supported configurations...........................................................................1

**Chapter 2. Planning...............................................................................3**

Roadmap....................................................................................................3
Prerequisites...............................................................................................4
Software downloads....................................................................................5
Installation worksheet.................................................................................5

**Chapter 3. Installing...............................................................................7**

Installing the dispatcher...............................................................................7
Installing the adapter binaries or connector..................................................8
Installing 3rd party client libraries.................................................................9
Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications.....................................................................................10
Configuring the SSL connection between IBM Security Directory Integrator and Aquera..........12
Verifying the adapter installation.................................................................14
Restarting the adapter service.....................................................................16
Importing the adapter profile.......................................................................17
Importing attribute mapping file..................................................................19
Adding a connector.....................................................................................20
Enabling connectors....................................................................................22
Reviewing and setting channel modes for each new connector....................24
Attribute Mapping.......................................................................................26
Creating an adapter service/target..............................................................28
Service/Target form details..........................................................................30
Adapter Details tab......................................................................................31
SAP Connection Details tab.........................................................................32
Reconciliation Advanced Mapping tab..........................................................32
Dispatcher Attributes tab.............................................................................32
Verifying that the adapter is working correctly.............................................33
Installing ILMT-Tags.....................................................................................34

**Chapter 4. Configuring.........................................................................37**

Suppressing password in clear text..............................................................37
Configuring Extended Schema.....................................................................37
Customizing the adapter profile...................................................................38
Modify the SCIM HR adapter profiles...........................................................39
customlabel.properties................................................................................39
schema.dsml...............................................................................................39
erTDIScimhrAccount.xml.............................................................................40
service.def..................................................................................................41
Importing the adapter profile jar..................................................................41

**Chapter 5. Troubleshooting....................................................................43**
Techniques for troubleshooting problems.......................................................43
Error messages and problem solving...........................................................44

**Chapter 6. Uninstalling.......................................................................47**
Deleting the adapter profile...................................................................47

**Chapter 7. Reference..........................................................................49**
Adapter attributes and object classes.........................................................49

**Index.........................................................................................55**

# Figures

1. The architecture of the SCIM HR adapter........1

2. Example of a single server configuration........2

3. Example of a multiple server configuration........2

# Tables

1. Prerequisites to install the adapter....4

2. Required information to install the adapter....5

3. Adapter components....14

4. Prerequisites for enabling a connector....22

5. Specific messages and actions....45

6. General messages and actions....45

7. Supported account attributes....49

8. USER_ERC attribute mapping....49

9. OrganizationalUnit_ERC attribute mapping....52

# Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The SCIM HR adapter enables communication between the Identity server and the SCIM HR Target.

## Features of the adapter

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

It checks the connection between the SCIM HR Application Server and IBM Security Verify Governance.

**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.

The adapter requires the following components:

- Dispatcher
- Security Directory Integrator connector
- SCIM HR adapter profile

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

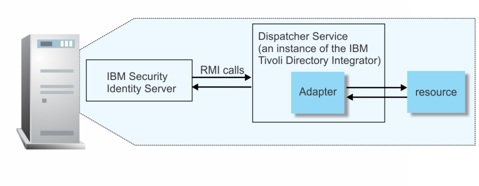
IBM Security Identity Server
RMI calls
Dispatcher Service (an instance of the IBM Tivoli Directory Integrator)
Adapter
resource

*Figure 1. The architecture of the SCIM HR adapter*

**Related concepts**

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

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 in each environment are:

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

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

## Single server configuration

In a single server configuration, the following components are installed in one server to establish communication with the SCIM HR resource server:

- Identity server
- Security Directory Integrator server
- SCIM HR adapter

The SCIM HR resource server is installed on a different server as shown in Figure 2 on page 2.

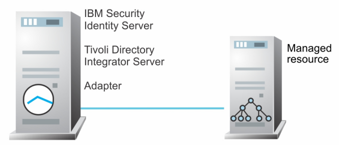

*Figure 2. Example of a single server configuration*

## Multiple server configuration

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

- Identity server
- Security Directory Integrator server
- SCIM HR adapter
- Managed resource

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

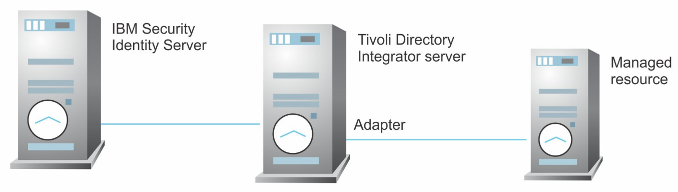

*Figure 3. Example of a multiple server configuration*

**Related concepts**

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

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.

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

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 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 1 on page 4 identifies the prerequisites for the adapter installation.

*Table 1. Prerequisites to install the adapter*

| Prerequisite | Description |
|---|---|
| Directory Integrator | • IBM® Security Directory Integrator Version 7.2 + FP6 + 7.2.0-ISS-SDI-LA0019 |

*Table 1. Prerequisites to install the adapter (continued)*

| Prerequisite | Description |
|---|---|
| Identity server | The following servers are supported:<br>• IBM Security Verify Governance Identity Manager v10.0<br>• IBM Security Verify Governance v10.0<br>• IBM Security Identity Manager v7.0.x<br>• IBM Security Identity Manager v6.0.x<br>• IBM Security Privileged Identity Manager v2.x<br>• IBM Security Identity Governance and Intelligence v5.2.x |
| Security Directory Integrator adapters solution directory | A Security Directory Integrator work directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*. |
| System administrator authority | You must have system administrator authority to complete the adapter installation procedure. |

## Software downloads

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

Go to IBM Passport Advantage. See the *IBM Security Verify Governance Download Document*.

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

## Installation worksheet

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

**Note:** Ensure that the adapter user is granted access to SNC.

*Table 2. Required information to install the adapter*

| Required information | Description | Value |
|---|---|---|
| Security Directory Integrator Home Directory | The *ITDI_HOME* directory contains the `jars/connectors` subdirectory, which contains the files for the adapters. | **Windows:**<br>• `*drive*\Program Files\IBM\TDI\V7.2`<br>**UNIX:**<br>• `/opt/IBM/TDI/V7.2` |
| Adapter Solution Directory | See the *Dispatcher Installation and Configuration Guide*. | **Windows:**<br>• `*drive*\Program Files\IBM\TDI\V7.2\*timsol*`<br>**UNIX:**<br>• `/opt/IBM/TDI/V7.2/*timsol*` |

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

| Required information | Description | Value |
|---|---|---|
| Create an API Client with a Client ID and a Client Secret on the SCIM HR resource | An API Client must be created with the required administrator access for provisioning and managing the user accounts on SCIM HR application. | |

# 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.

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

## Installing the dispatcher

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

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

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

**Related concepts**

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

# Installing the adapter binaries or connector

The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

- The Dispatcher must be installed.

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**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing 3rd party client libraries

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## Installing 3rd party client libraries

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

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications

To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

For more information about SSL configuration between the Dispatcher and the Identity Server, see the *Dispatcher Installation and Configuration Guide*.

1. On a web browser, go to your SCIM Instance URL. For example, `https://<domain_name>`.
2. View the certificate.
   a) Click the SSL lock icon on the browser.

b) If your browser reports that the revocation information is not available, click **View Certificates**.

3. On the Certificate window, open the **Certification Path** tab and select **Root CA or domain certificates**. This depends on the SCIM domain instance.
4. Open the Details tab and click Copy to File.
5. In the Certificate Export Wizard, select the **Base-64 encoded X.509 (.CER)** format.
6. Perform one of the following actions:

   - If the RMI Dispatcher already has a configured keystore, use the keytool.exe program to import the IBM Security Verify Adapter for SCIM Adapter server certificate.
   - If the keystore is not yet configured, create it by running the following command from a command prompt.

     Type the command on a single line.

     ```
     keytool -import -alias scimcert -file c:\scim_cert.cer -keystore
     truststore.jks -storepass passw0rd
     ```
7. Optional: Edit `IDI_HOME/timsol/solution.properties` file to specify the truststore and keystore information.

   **Note:**

   In the current release, only jks-type is supported:

   - Keystore file information for the server authentication
   - It is used to verify the server public key. For example,
     - `javax.net.ssl.trustStore=truststore.jks`
     - `javax.net.ssl.trustStorePassword=passw0rd`
     - `javax.net.ssl.trustStoreType=jks`

   If these key properties are not configured, you can set truststore to the same that contains the target resource server certificate. Otherwise, you must import the target resource certificate to the truststore specified in `javax.net.ssl.trustStore`.
8. Update the `log4j.properties` file. Locate the `log4j.properties` file under the solution directory (`timsol`) and make the following changes:

   - Add: `log4j.logger.org.apache.http=ERROR, Default`
   - Add: `log4j.rootCategory=INFO, Default`
9. After you modify the `log4j.properties` file, restart the Dispatcher. For information about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

Service/Target form details

Complete the service/target form fields.

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## Configuring the SSL connection between IBM Security Directory Integrator and Aquera

To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

1. On a web browser, navigate to the Aquera Instance URL: https://admin.aquera.io/home/login.
2. View the certificate.
   a) Click the SSL lock icon on the browser.
   b) Go to **Certificate is valid**.
3. In the Certificate window, open the **Certification Path** tab and select **Starfield class 2 Certification Authority**.
4. Click **View certificates**, open the **Details** tab and click on **Copy to file**.

5. In the Certificate Export Wizard, select the **Base-64 encoded X.509 (.CER)** format.
6. Perform one of the following actions:

   - If the RMI Dispatcher already has a configured keystore, use the keytool.exe program to import the IBM Security Verify Adapter for SCIM Adapter server certificate.
   - If the keystore is not yet configured, create it by running the following command from a command prompt.

     Type the command on a single line.

     ```
     keytool -import -alias scimcert -file c:\scim_cert.cer -keystore
     truststore.jks -storepass passw0rd
     ```
7. Optional: Edit `IDI_HOME/timsol/solution.properties` file to specify the truststore and keystore information.

   **Note:**

   In the current release, only jks-type is supported:

   - Keystore file information for the server authentication
   - It is used to verify the server public key. For example,
     - `javax.net.ssl.trustStore=truststore.jks`
     - `javax.net.ssl.trustStorePassword=passw0rd`
     - `javax.net.ssl.trustStoreType=jks`

   If these key properties are not configured, you can set truststore to the same that contains the target resource server certificate. Otherwise, you must import the target resource certificate to the truststore specified in `javax.net.ssl.trustStore`.
8. Update the `log4j.properties` file. Locate the `log4j.properties` file under the solution directory (`timsol`) and make the following changes:

   - Add: `log4j.logger.org.apache.http=ERROR, Default`
   - Add: `log4j.rootCategory=INFO, Default`
9. After you modify the `log4j.properties` file, restart the Dispatcher. For information about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector

The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

# Verifying the adapter installation

After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

*Table 3. 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 |
| *ITDI_HOME*/libs | sapjco3.dll |

*Table 3. Adapter components (continued)*

| **Directory** | **Adapter component** |
|---|---|
| *ITDI_HOME*/solution/xsl | • sapnw_bapi_errors.properties<br>• sapnw_bapi_person_getdetail_precall.xsl<br>• sapnw_bapi_person_address_precall.xsl<br>• sapnw_bapi_person_email_precall.xsl<br>• sapnw_bapi_person_getdetail_postcall.xsl |

**Related concepts**

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

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

# Restarting the adapter service

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

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

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

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## 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.

- 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.

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 server can manage.

The adapter profile definition file is used to create a target profile on the Verify Governance 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:

1. Log in to the Verify Governance 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.

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.

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

- Import the attribute mapping file. See "Importing attribute mapping file" on page 19.
- Create a connector that uses the target profile. See "Adding a connector" on page 20.

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

# Importing attribute mapping file

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

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.

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

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## Adding a connector

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

Complete Importing the adapter profile.

**Note:** If you migrated from Verify Governance 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 product documentation.

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.

To add a connector, complete these steps.

1. Log in to the Verify Governance 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.

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.

Enable the channel modes to synchronize the data between the target systems and Verify Governance. For more information, see “Enabling connectors” on page 22.

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

Service/Target form details

Complete the service/target form fields.

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## Enabling connectors

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

*Table 4. Prerequisites for enabling a connector*

| Prerequisite | Find more information |
|---|---|
| A connector must exist in Verify Governance. | "Adding a connector" on page 20. |
| Ensure that you enabled the appropriate channel modes for the connector. | "Reviewing and setting channel modes for each new connector" on page 24. |

To enable a connector, complete these steps:

1. Log in to the Verify Governance 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.

The connector is enabled

Enable the channel modes to synchronize the data between the target systems and Verify Governance.

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications

To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## 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.

**Note:** Legacy Verify Governance 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.

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 V5.2.3:

1. Log in to the Verify Governance 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 22.

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

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

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector

The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the user or OU attributes.

Files in /Users/ibmuser/FileNet/Work/Current/IDCMS1/TIV/v_adapters/6.0/im60/common

t_map_adap_attrs_acct_igi_5.2.3.dita - OK

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

The file consists of

Files in /Users/ibmuser/FileNet/Work/Current/IDCMS1/TIV/v_adapters/6.0/im60/common

t_map_adap_attrs_acct_igi_5.2.3.dita - OK

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

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

```
GIVEN_NAME=ersaphrgivenname
```

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

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

**Note:**

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

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 attribute values.

   Files in /Users/ibmuser/FileNet/Work/Current/IDCMS1/TIV/v_adapters/6.0/im60/common

   t_map_adap_attrs_acct_igi_5.2.3.dita - OK

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

   For example:

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

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

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

   ```

   [conversion.date].ersaphrdob.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 product documentation.

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

Restarting the adapter service

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## 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.

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

repackage the JAR file with the updated files. The JAR file for IBM Security Verify Governance is located in the top level folder of the installation package

You must create an administrative user account for the adapter on the managed resource. Provide the account information 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, 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.

1. Log in to the Identity server as an administrator.
2. In the **MyWork** pane, click **Manage Services** > **Create**.
3. In the **Select the Type of Service** page, select **SCIM service**.
4. Click **Next** to display the adapter service form.

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

# Service/Target form details

Complete the service/target form fields.

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

- "Adapter Details tab" on page 31
- "SAP Connection Details tab" on page 32
- "Reconciliation Advanced Mapping tab" on page 32
- "Dispatcher Attributes tab" on page 32

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications

To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

## Adapter Details tab

This tab describes service details.

**Service name**
Specify a name that defines this service on the IBM Security Verify Governance 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, `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 the parameters that have to be specified to establish a remote connection to the SCIM HR resource from IBM Security Directory Integrator.

**Target Client**
The SAP instance client number. This field is mandatory.

**Login ID**
The SAP User account login ID that adapter uses to connect to the SAP instance. This field is mandatory.

**Password**
Password for SAP User account. This field is mandatory.

**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.

**SAP Systems Number**
The SAP server system number. This field is mandatory.

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

## Reconciliation Advanced Mapping tab

Settings in this tab apply only during reconciliation and search operation requests.

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

- Search Person Basic Iterate Request XSL Stylesheets
- Search Person 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 that are received from IBM Security Verify Governance.

For example:

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

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

**Max Connection Count**

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

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

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

**Disable Assembly Line Cache**

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

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

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

## Verifying that the adapter is working correctly

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

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

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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.

Installing ILMT-Tags
This topic describes the procedures to install ILMT tag files.

# Installing ILMT-Tags

This topic describes the procedures to install ILMT tag files.

Ensure that the Dispatcher is installed.

- Copy the files from **ILMT-Tags** folder to the specified location:
  - Windows: `<SDI-HOME>/swidtag`
  - Unix/Linux: `<SDI-HOME>/swidtag`

**Related concepts**

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

Verifying the adapter installation
After you install the adapter, verify the adapter components on the IBM Security Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

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

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

**Related tasks**

Installing the adapter binaries or connector
The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Installing 3rd party client libraries

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

Configuring the SSL connection between the IBM Security Directory Integrator and the SCIM applications
To enable SSL connection between the adapter and the IBM Security Verify Adapter for SCIM Adapter server, configure the keystores for the Dispatcher.

Configuring the SSL connection between IBM Security Directory Integrator and Aquera
To enable SSL connection between the adapter and the Aquera, configure the keystores for the Dispatcher.

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 server, add a connector so that Verify Governance 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 user or OU attributes.

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. 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

## Suppressing password in clear text

The REST API shows the password in clear text when you are executing the user add and password change operations. This section provides information to suppress the password in clear text.

1. Add the following property to the `log4j properties` file:

   ```
   log4j.logger.org.apache.http=ERROR, Default
   ```

   **Note:** The property must be added after the following property:

   ```
   log4j.rootCategory=DEBUG, Default
   ```

2. Restart the Dispatcher.

**Related concepts**

Modify the SCIM HR adapter profiles
Modify the SCIM HR adapter profiles with the instructions listed in this section.

**Related tasks**

Configuring Extended Schema
This topic provides information on how to configure extended schema.

Customizing the adapter profile
To customize the adapter profile, you must modify the SCIMHR Adapter JAR file and ScimHRAdapterProfile.jar. Files need to be customized to perform the provisioning from IBM Security Verify Governance.

Importing the adapter profile jar
After editing the SCIM HR adapter profile jar, you must import the file into the IBM Security Verify server for the changes to take effect.

## Configuring Extended Schema

This topic provides information on how to configure extended schema.

Create a .txt file to key in the extended schema attributes of SCIM HR target.

**Service form**
Obtain the mapping file location from the service form.

**Extended Schema File Path**
`{SDI_HOME}/timsol/ SampleSchemaAttrMapping.txt`

The adapter reads the .txt file from the service form and segregate the schema and the schema related attributes.

**SampleSchemaAttrMapping.txt**

Supply the schema attribute mapping file to enable support for the extended schema. Use the following mapping file format:

```
urn:ietf:params:scim:schemas:extension:hcl:2.0:User //schema1
erAttribute|attribute
erAttribute1|attribute1
urn:ietf:params:scim:schemas:extension:ibm:2.0:User //schema2
erAttribute2|attribute2
```

The adapter supports the following attribute structure:

```
endpoint:/Entitlements|id:erEntitlementid|displayName:erEntitlementDisplayName
|value:erscimentitlementmember|objectclass:erEntitlementclass
```

**Related concepts**

Modify the SCIM HR adapter profiles
Modify the SCIM HR adapter profiles with the instructions listed in this section.

**Related tasks**

Suppressing password in clear text
The REST API shows the password in clear text when you are executing the user add and password change operations. This section provides information to suppress the password in clear text.

Customizing the adapter profile
To customize the adapter profile, you must modify the SCIMHR Adapter JAR file and ScimHRAdapterProfile.jar. Files need to be customized to perform the provisioning from IBM Security Verify Governance.

Importing the adapter profile jar
After editing the SCIM HR adapter profile jar, you must import the file into the IBM Security Verify server for the changes to take effect.

## Customizing the adapter profile

To customize the adapter profile, you must modify the SCIMHR Adapter JAR file and ScimHRAdapterProfile.jar. Files need to be customized to perform the provisioning from IBM Security Verify Governance.

The adapter JAR file includes the following files:

- `CustomLabels.properties`
- `erTDIScimhAccount.xml`
- `schema.dsml`
- `service.def`
- `targetProfile.json`

1. Copy the SCIM HR profile JAR file into a temporary directory.
2. Extract the contents of the JAR file into the temporary directory by running the following command:

   ```
   cd c:\temp
    jar -xvf ScimHRAdapterProfile.jar
   ```

   The jar command extracts the files into the directory.
3. Edit the file accordingly.

**Related concepts**

Modify the SCIM HR adapter profiles

Modify the SCIM HR adapter profiles with the instructions listed in this section.

**Related tasks**

Suppressing password in clear text
The REST API shows the password in clear text when you are executing the user add and password change operations. This section provides information to suppress the password in clear text.

Configuring Extended Schema
This topic provides information on how to configure extended schema.

Importing the adapter profile jar
After editing the SCIM HR adapter profile jar, you must import the file into the IBM Security Verify server for the changes to take effect.

# Modify the SCIM HR adapter profiles

Modify the SCIM HR adapter profiles with the instructions listed in this section.

**Related tasks**

Suppressing password in clear text
The REST API shows the password in clear text when you are executing the user add and password change operations. This section provides information to suppress the password in clear text.

Configuring Extended Schema
This topic provides information on how to configure extended schema.

Customizing the adapter profile
To customize the adapter profile, you must modify the SCIMHR Adapter JAR file and ScimHRAdapterProfile.jar. Files need to be customized to perform the provisioning from IBM Security Verify Governance.

Importing the adapter profile jar
After editing the SCIM HR adapter profile jar, you must import the file into the IBM Security Verify server for the changes to take effect.

## customlabel.properties

Modify the `customlabel.properties` by adding entitlements.

- Add the following entitlements to the `customlabel.properties` file:

```
#entitlements
erentitlementid=Entitlement Id
erentitlementdisplayname=Entitlement Name
erscimentitlementmember=Entitlement Member
erscimentitlementdescription=Entitlement Description
```

## schema.dsml

Modify the `schema.dsml` file by adding all the entitlements attributes under the `erentitlementclass`.

- Add the following entitlements attributes under the `erentitlementclass` in the `schema.dsml`:

```
<!-- **************************************************************    -->
        <!-- erEntitlementclass                                             -->
        <!-- ************************************************************** -->
        <class superior="top">
        <name>erEntitlementclass</name>
        <description>Scim group class</description>
        <object-identifier>1.3.6.1.4.1.6054.3.193.1.3</object-identifier>
        <attribute ref = "erEntitlementid" required = "true" />
        <attribute ref = "erEntitlementDisplayName" required = "false" />
        <attribute ref = "erscimentitlementdescription" required = "false" />
        </class>
```

- Add the following entitlement attributes (erentitlementid, erentitlementDisplayName,erentitlementmember) under the attribute:

```
<!-- ******************************************************** -->
        <!-- erEntitlementid                                  -->
        <!-- ******************************************************** -->
        <attribute-type single-value = "true" >
            <name>erEntitlementid</name>
            <description>Entitlementid</description>
            <object-identifier>1.3.6.1.4.1.6054.3.193.2.27</object-identifier>
            <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
        </attribute-type>

        <!-- ******************************************************** -->
        <!-- erEntitlementDisplayName                                  -->
        <!-- ******************************************************** -->
        <attribute-type single-value = "true" >
            <name>erEntitlementDisplayName</name>
            <description>EntitlementDisplayName</description>
            <object-identifier>1.3.6.1.4.1.6054.3.193.2.28</object-identifier>
            <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
        </attribute-type>

        <!-- ******************************************************** -->
        <!-- erscimentitlementmember                                  -->
        <!-- ******************************************************** -->
        <attribute-type single-value = "true" >
            <name>erscimentitlementmember</name>
            <description>Member</description>
            <object-identifier>1.3.6.1.4.1.6054.3.193.2.29</object-identifier>
            <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
        </attribute-type>
```

- Add the erentitlementmember in the erTDIhrAccountclass.

```
<!--******************************************************** -->
<!--erTDIScimhrAccount Class-->
<!--******************************************************** -->
<class superior="top"><name>erTDIScimhrAccount</name>
<description>SCIM HR Feed Account class</description>
<object-identifier>1.3.6.1.4.1.6054.3.193.1.2</object-identifier>
<attribute ref = "eruid" required = "true" />
<attribute ref = "erAccountStatus" required = "false" />
<attribute ref = "erscimhrgivenname" required = "false" />
<attribute ref = "erscimhrsurname" required = "false" />
<attribute ref = "erscimhrEmailWork" required = "false" />
<attribute ref = "erscimhrworkphonenumber" required = "false" />
<attribute ref = "erscimhraddress" required = "false" />
<attribute ref = "erscimhrcity" required = "false" />
<attribute ref = "erscimhrpostalCode" required = "false" />
<attribute ref = "erscimhrcountry" required = "false" />
<attribute ref = "erscimentitlementmember" required = "false" />
</class>
```

## erTDIScimhrAccount.xml

Modify the erTDIScimhrAccount.xml file by modifying the formelement for erentitlementclass.

- Modify the formelement for erentitlementclass.

```
<formElement name="data.erscimentitlementmember" label="$erscimentitlementmember">
   <searchFilter multiple="true" type="select">
   <filter>(objectclass&#61;erentitlementclass)</filter>
   <base>contextual</base>
   <attribute>erentitlementdisplayname</attribute>
<size></size>
   <objectClass></objectClass>
   <paginateResults>false</paginateResults>
</searchFilter>
</formElement>
```

### service.def

Modify the `service.def` file by modifying the `serviceGroups` and Attribute map for the entitlements.

- Modify the `serviceGroups` and Attribute map for the entitlements.

```
<ServiceGroups>
     <GroupDefinition profileName="SCIMGroupHRProfile"
            className = "erentitlementclass"
            rdnAttribute = "erentitlementid"
            accountAttribute = "erscimentitlementmember">
        <AttributeMap>
                <Attribute name = "erGroupId" value="erentitlementid"/>
                <Attribute name = "erGroupName"  value= "erentitlementdisplayname"/>
                <Attribute name="erGroupDescription" value="erentitlementdisplayname"/>
            </AttributeMap>
        </GroupDefinition>
</ServiceGroups>
```

## Importing the adapter profile jar

After editing the SCIM HR adapter profile jar, you must import the file into the IBM Security Verify server for the changes to take effect.

1. Create a JAR file with the files in the `\temp` directory by running the following command:

```
cd c:\temp jar -cvf
ScimHRAdapterProfile.jar ScimHRAdapterProfile
```

2. Import the JAR file into the IBM Security Verify Governance server.
3. Stop and start the IBM Security Verify server.
4. Restart the adapter service.

**Related concepts**

Modify the SCIM HR adapter profiles
Modify the SCIM HR adapter profiles with the instructions listed in this section.

**Related tasks**

Suppressing password in clear text
The REST API shows the password in clear text when you are executing the user add and password change operations. This section provides information to suppress the password in clear text.

Configuring Extended Schema
This topic provides information on how to configure extended schema.

Customizing the adapter profile
To customize the adapter profile, you must modify the SCIMHR Adapter JAR file and ScimHRAdapterProfile.jar. Files need to be customized to perform the provisioning from IBM Security Verify Governance.

# Chapter 5. Troubleshooting

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

## Techniques for troubleshooting problems

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

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

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

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

### What are the symptoms of the problem?

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

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

### Where does the problem occur?

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

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

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

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

### When does the problem occur?

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

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

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

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

### Under which conditions does the problem occur?

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

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

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

### Can the problem be reproduced?

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

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

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

## Error messages and problem solving

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

Table 5 on page 45 and Table 6 on page 45 contain warnings or errors, which might be displayed when the SCIM HR adapter is installed on your system.

*Table 5. Specific messages and actions*

| Message number | Message | Action |
|---|---|---|
| CTGIMT600E | An error occurred while establishing communication with the IBM Security Directory Integrator server. | • Verify that the IBM Security Directory Integrator-based adapter service is running.<br>• Verify that the URL specified on the service form for IBM Security Directory Integrator is correct. |
| CTGIMT001E | The following error occurred.<br>Error during authentication. Ensure Client ID, Client Secret, and the SCIM HR URL is correct | • Verify that the SCIM HR Target URL is running.<br>• Verify that the SCIM HR client ID and client secret that is specified on the service form of the SCIM HR Target are correct. |
| CTGIMU107W | The following error occured:<br>Test Connection Fails: The connection to the specified service cannot be established. | Verify the service information and try again.<br>**ibmdi.log**<br>The service name might contain special characters that IBM Security Directory Integrator can not handle. For example, "/". |

*Table 6. General messages and actions*

| Message | Action |
|---|---|
| `java.lang.NoClassDefFoundError: org.apache.http.client.ClientProtocolException` | The `httpclient-4.5.2.jar` file is missing. Verify that the file exists in the *`ITDI_HOME`*`/jars/3rdParty/IBM` directory. |
| `Adapter profile is not displayed in the user interface after installing the profile.` | You must stop and restart the Security Directory Integrator server or wait until the cache times out (up to 10 minutes) for IBM Security Verify Governance to refresh the list of attribute names. |

# Chapter 6. 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.

1. Stop the IBM Security Verify Governance Dispatcher Service.
2. Remove the SCIM HR adapter JAR files.
   a. Delete `ScimConnector.jar` and `scimconnector.jar` from the *`ITDI_HOME`*`/jars/connectors` directory.
   b. Delete `SapNWRfc.jar` from the *`ITDI_HOME`*`/jars/functions` directory.

      **Note:** If you are using this IBM Security Directory Integrator to provision to a SAP NetWeaver target then do not delete the`scimconnector.jar` and `SapNWRfc.jar`.
3. Remove the adapter stylesheets from the *`ITDI_HOME`*`/`*`solution`*`/xsl` directory.
4. Delete the adapter profile from the Identity server.

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

## Deleting the adapter profile

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

Objects on the Identity server that can reference the adapter profile:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

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

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

# Chapter 7. Reference

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

## Adapter attributes and object classes

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

The SCIM HR adapter supports a standard set of attributes.

*Table 7. Supported account attributes*

| Attribute Name | Description | Required |
|---|---|---|
| **erScimHRCredUserName** | Username | YES |
| **erscimhrgivenname** | Given name | YES |
| **erscimhrsurname** | Surname | YES |
| **erscimhrdisplayname** | Display name | NO |
| **erscimhrEmailWork** | Work email | YES |
| **erscimhrlastname** | Formatted name | NO |
| **erscimhrworkphonenumber** | Work phone number | NO |
| **erscimhrmobilephonenumber** | Mobile phone number | NO |
| **erscimhrcity** | City | NO |
| **erscimhraddress** | Address | NO |
| **erscimhrpostalCode** | Postal Code | NO |
| **erscimhrcountry** | Country | NO |
| **erscimhrzipcode** | Zip Code | NO |

### USER_ERC attribute mapping

The following table lists which adapter attributes are mapped to the attributes stored in the IBM Security Verify Governance USER_ERC table.

*Table 8. USER_ERC attribute mapping*

| USER_ERC attributes | Description | Required | SCIM HR adapter attribute name |
|---|---|---|---|
| ID | Table unique identifier.<br>The sequence `user_erc_seq` might be called to generate this unique number. | YES | |

*Table 8. USER_ERC attribute mapping (continued)*

| USER_ERC attributes | Description | Required | SCIM HR adapter attribute name |
|---|---|---|---|
| PM_CODE | USER ID or User Code.<br>It is not required. USER ID can be generated using a rule. | NO | |
| OU | Organizational unit code.<br>Used to store the user in the OU available in the system.<br>This attribute might or might not be in the database. Create the new OU in the `root`. | YES | **ersaphrpersonou** |
| USER_TYPE | User type name.<br>This attribute might or might not be in the database. It can be created dynamically using a custom rule. | NO | |
| PROCESSED | Deprecated | NO | |
| LAST_MOD_USER | Contains the name of the last user or process that modified the USER_ERC table. | NO | |
| LAST_MOD_TIME | Contains the date and time when the last change occurred.<br>Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed. | NO | |
| POST_EVENT | Deprecated | NO | |
| SKIP | Deprecated | NO | |
| ACTION_TYPE | SAP HR property information. | NO | |
| ACTION_CAUSE | SAP HR property information. | NO | |
| ACTION_TYPE_LAST | SAP HR property information. | NO | |
| ACTION_CAUSE_LAST | SAP HR property information. | NO | |
| GIVEN_NAME | User name | YES | **ersaphrgivenname** |
| SURNAME | User surname | YES | **ersaphrlastname** |

*Table 8. USER_ERC attribute mapping (continued)*

| USER_ERC attributes | Description | Required | SCIM HR adapter attribute name |
|---|---|---|---|
| GENDER | - 0 = male<br>- 1 = female | NO | **ersaphrgender** |
| BIRTHDAY | Birthday | NO | **ersaphrdob** |
| BIRTH_PLACE | Birth place | NO | **ersaphrbirthplace** |
| BIRTH_COUNTRY | Birth country | NO | **ersaphrbirthcountry** |
| ACCOUNT_EXPIRY_DATE | The Verify Governance account can be created with an expiration date.<br>Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed. | NO | |
| IDENTIFICATION_NUMBER | User ID present into HR system | NO | **eruid** |
| CURRENTOU | Deprecated | NO | |
| NATION | Nation | NO | |
| ZIPCODE | Zip code | NO | **ersaphrzipcode** |
| COUNTRY | Country | NO | **ersaphrcountry** |
| PHONE_NUMBER | Phone number | NO | **ersaphrphoneno** |
| DISABLED | Indicates that the user is disabled and it disables all user accounts | NO | |
| DELETED | Use this attribute to implement a particular logic when a user is deleted from HR system.<br>For example, a user can keep all his account for 3 weeks and then the user is deleted | NO | |
| ATTR1 | Spare attribute | NO | |
| ATTR2 | Spare attribute | NO | |
| ATTR3 | Spare attribute | NO | |
| ATTR4 | Spare attribute | NO | |
| ATTR5 | Spare attribute | NO | |
| ATTR6 | Spare attribute | NO | |
| ATTR7 | Spare attribute | NO | |
| ATTR8 | Spare attribute | NO | |
| ATTR9 | Spare attribute | NO | |

*Table 8. USER_ERC attribute mapping (continued)*

| USER_ERC attributes | Description | Required | SCIM HR adapter attribute name |
|---|---|---|---|
| ATTR10 | Spare attribute | NO | |
| ATTR11 | Spare attribute | NO | |
| ATTR12 | Spare attribute | NO | |
| ATTR13 | Spare attribute | NO | |
| ATTR14 | Spare attribute | NO | |
| ATTR15 | Spare attribute | NO | |
| SCHEDULE | Deprecated | NO | |
| ADDRESS | User address | NO | **ersaphraddress** |
| CITY | User city | NO | **ersaphrcity** |
| EMAIL | User email | NO | **ersaphremailid** |

## OrganizationalUnit_ERC attribute mapping

The following table lists which adapter attributes are mapped to the attributes stored in the IBM Security Verify Governance OrganizationalUnit_ERC table.

*Table 9. OrganizationalUnit_ERC attribute mapping*

| OrganizationalUnit_ERC attributes | Description | Required | SCIM HR adapter attribute name |
|---|---|---|---|
| ID | Table unique identifier.<br>The sequence `organizational_unit_erc_seq` might be called to generate this unique number. | YES | |
| PARENT | Organizational unit parent code<br>This attribute might or might not be in the database. Create the new OU in the `root`. | NO | |
| OU | Organizational unit code (unique identifier) | YES | **ersaphrorgid** |
| DESCRIPTION | Description | NO | **ersaphrorgdesc** |
| NAME | Organizational unit name | YES | **ersaphrorgname** |
| LAST_MOD_USER | Contains the name of the last user or process that modified the USER_ERC table. | NO | |

*Table 9. OrganizationalUnit_ERC attribute mapping (continued)*

| OrganizationalUnit_ERC attributes | Description | Required | SCIM HR adapter attribute name |
|---|---|---|---|
| LAST_MOD_TIME | Contains the date and time when the last change occurred.<br>Default format is `dd/MM/yyyy HH:mm:ss`. Format can be changed. | NO | |
| TIPO | Organizational unit type name.<br>This attribute might or might not be in the database. It can be created dynamically using a custom rule. | NO | |
| SCHEDULE | Deprecated | NO | |
| ATTR1 | Spare attribute | NO | |
| ATTR2 | Spare attribute | NO | |
| ATTR3 | Spare attribute | NO | |
| ATTR4 | Spare attribute | NO | |
| ATTR5 | Spare attribute | NO | |
| ATTR6 | Spare attribute | NO | |
| ATTR7 | Spare attribute | NO | |
| ATTR8 | Spare attribute | NO | |
| ATTR9 | Spare attribute | NO | |
| ATTR10 | Spare attribute | NO | |
| ATTR11 | Spare attribute | NO | |
| ATTR12 | Spare attribute | NO | |
| ATTR13 | Spare attribute | NO | |
| ATTR14 | Spare attribute | NO | |
| ATTR15 | Spare attribute | NO | |

# Index

## A

account
  management automation 1
adapter
  account management automation 1
  customization steps 38
  details tab, attributes 31
  features 1
  installation 7
  profile
    removal 47
  uninstall 47
after installation 37
automation, account management 1

## D

dispatcher
  installation 7
Dispatcher 1
download, software 5

## E

error messages 44

## F

first steps 37

## I

installation
  adapter 7
  preparation 3
  troubleshooting 43
  uninstall 47
  verify 14

## M

messages
  error 44
  warning 44

## P

profile
  removal 47

## R

reconciliation
  advanced mapping tab, service attribute 32

## S

SAP connection details tab, attributes 32
service
  restart 16
  start 16
  stop 16
software
  download 5
  website 5

## T

tivoli directory integrator connector 1
troubleshooting
  adapter installation 43
  error messages 44
  identifying problems 43
  techniques for 43
  warning messages 44
troubleshooting and support
  troubleshooting techniques 43

## U

uninstallation 47
updating
  adapter profile 38

## V

verification
  dispatcher installation 7
  installation 14

## W

warning messages 44