IBM Security Verify Governance Identity Manager
10.0

IBM Security Verify Adapter for SCIM Adapter Installation and Configuration Guide

Contents

Figures

Tables

Overview

An adapter is an interface between a managed resource and the Identity server. The IBM Security Verify Adapter for SCIM Adapter enables communication between the Identity server and the IBM Security Verify Adapter for SCIM Adapter server.

SCIM Identity IBM Security Verify Governance Identity Manager server manages access to the resource. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions the administrators can run manually.

The adapter runs as a service, independent of whether you are logged on to the IBM Security Verify Governance Identity Manager server.

Features of the adapter

The adapter automates several administrative and management tasks.

The adapter supports the following tasks:

- Reconciling user accounts and support data, such as groups.
- Adding and modifying user accounts
- Modifying user account attributes
- Modifying user account password
- Suspending and restoring user accounts
- Checking the connection between the IBM Security Verify Adapter for SCIM Adapter server and IBM Security Verify Governance Identity Manager server.

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 Adapter profile

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

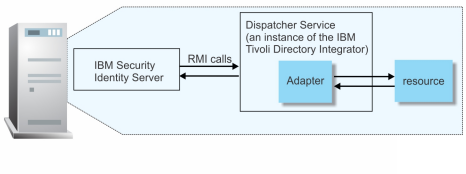

Figure 1. The architecture of the IBM Security Verify Adapter for SCIM Adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

- The Identity server
- The IBM Security Directory Integrator server

- The managed resource
- SCIM Adapter

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

Single server configuration

In a single server configuration, the following components are installed on one server to establish communication with the IBM Security Verify Adapter for SCIM Adapter server:

- Identity server
- Security Directory Integrator server
- SCIM Adapter

The IBM Security Verify Adapter for SCIM Adapter server is installed on a different server as shown in Figure 2 on page x.

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 Adapter
- Managed resource

TheSecurity Directory Integrator server and the IBM Security Verify Adapter for SCIM Adapter are installed on the same server as shown in Figure 3 on page x.

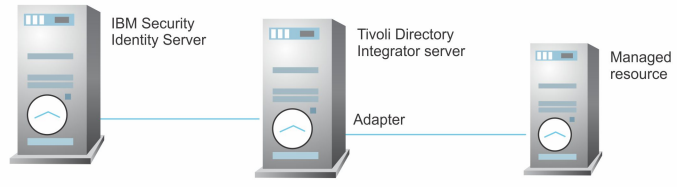

Figure 3. Example of a multiple server configuration

Planning

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

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.x

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

5. Customize the adapter.

Troubleshooting

See the following topics.

- Techniques for troubleshooting problems
- Configure debugging
- Logs
- Error messages and problem solving

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Related concepts

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

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

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

Prerequisites

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

Table 1 on page xii 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: • IBM Security Identity Manager server Version 6.0 • IBM Security Identity Manager server Version 7.0 • IBM Security Identity Governance and Intelligence v5.2.x • IBM Security Verify Governance Identity Manager v10.0.x • IBM Security Verify Governance v10.0.x
IBM Security Directory Integrator adapters solution directory	A IBM Security Directory Integrator working directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*.
System administrator authority	You must have system administrator authority to complete the adapter installation procedure.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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

Software downloads

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

Go to IBM Passport Advantage.

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

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

Installation worksheet

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

Installation worksheet

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

Table 2. Required information to install the adapter

Required information	Description	Value
IBM Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory, which contains the files for the adapters.	**Windows:** *drive*`\Program Files\IBM\TDI\V7.2\timsol` **UNIX:** `/opt/IBM/TDI/V7.2`
Adapter Solution Directory	When you install the dispatcher, the installer prompts you to specify a filepath for the solution directory. For more information, see the *Dispatcher Installation and Configuration Guide*.	**Windows:** *drive*`\Program Files\IBM\TDI\V7.2\timsol` **UNIX:** `/opt/IBM/TDI/V7.2/`
Create an API Client with a Client ID and a Client Secret on the SCIM resource	An API Client must to be created with the required administrator access for provisioning and managing the user accounts on IBM Security Verify Adapter for SCIM Adapter server. Click **Configuration** > **API Access** tab on the resource with client ID and Client secret to create an API client.	

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager 10.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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

Installing

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

Installing the dispatcher

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

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

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

Related concepts

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

Verifying that the adapter is working correctly

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

Installing the adapter binaries or connector

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

The Dispatcher must be installed..

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `ScimConnector.jar` file from the adapter package to the `ITDI_HOME/jars/connectors` directory.
4. Restart the adapter service.

Related concepts

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

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

Verifying that the adapter is working correctly

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

Installing third-party client libraries

The adapter requires access to the following jars at runtime.

Download Jars listed below and copy them to the Security Directory Integrator environment:

- `httpclient-4.5.2.jar`

  Download the `httpclient-4.5.2.jar` from https://mvnrepository.com/artifact/org.apache.httpcomponents/httpclient/4.5.2.
- `httpcore-4.4.4.jar`

  Download the `httpcore-4.4.4.jar` from https://mvnrepository.com/artifact/org.apache.httpcomponents/httpcore/4.4.4.
- `json-simple-1.1.1.jar` from

  Download the `json-simple-1.1.1.jar` from http://central.maven.org/maven2/com/googlecode/json-simple/json-simple/1.1.1/.

  .

1. Download the above-mentioned JAR files. Copy the files into `ITDI_HOME\jars\3rdparty\others` directory.

   Note: If there are issues with `NoClassDefFoundError`, copy the files into `SDI_HOME\jars\patches` instead of `SDI_HOME\jars\3rd party\others`.
2. Restart the Dispatcher service once all JAR files are placed under `ITDI_HOME\jars\3rdparty\others` directory.

   For information about starting and stopping the service, 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
If the adapter is installed correctly, the `ScimConnector.jar` file exists in the specified directory.

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

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

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

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.

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

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

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

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details

This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

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

Verifying the adapter installation

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

Windows operating system

drive`:\Program Files\IBM\TDI\7.2\jars\connectors\`

UNIX operating system

`/opt/IBM/TDI/7.2/jars/connectors/`

If the adapter is installed correctly, the following jars are seen in `ITDI_HOME\jars\3rdparty\others` directory:

- `httpclient-4.5.2.jar`
- `httpcore-4.4.4.jar`
- `json-simple-1.1.1.jar`

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

Related concepts

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details

This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

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

Restarting the adapter service

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

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

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

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

Related concepts

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

Installing the adapter binaries or connector

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

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

Importing the adapter profile

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

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

Service definition files are also called adapter profile files.

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

Profiles contained in this package

In the V7.1.15 and later installation package, the following profiles are included:

- IBM Security Verify Governance
- Governance Data Integration
- IBM Security Verify Governance Identity Manager

Installing the IBM Security Verify Governance Identity Manager specific version on an IBM Security Verify Governance Identity Manager server removes the requirement to install the Complex Attribute Handler. This can be of interest when you have defined policies on the IBM Security Verify Governance Identity Manager server that manage `ertopzprofile` related processing.

If no customization is done to the IBM Security Verify Governance Identity Manager server that involves the `ertopzprofile` attribute, the IBM Security Verify Governance profile can be used in

combination with the Complex Attribute Handler on IBM Security Verify Governance Identity Manager servers.

For the Governance Data Integration profile the complex attribute handler is not required. It merely defines the Top Secret Profile object class as a Service Group for IBM Security Verify Governance compatibility. This profile can be used if Top Secret profile assignments are made from IBM Security Verify Governance.

To make changes in the Top Secret profile assignments in both IBM Security Verify Governance and IBM Security Verify Governance Identity Manager,modify the `resource.def` file that is included in the profile jar to define the `ertopzprofile` attribute as complex attribute and the following complex attribute handler properties.

```
<Property Name = "ercomplexattributes" Value = "ertopzprofile" />
<Property Name = "erattributehandler" Value =
"com.ibm.isim.util.complexattribute.TopSecretComplexAttributeHandler" />
```

Then include the complex attribute handler jar file in the `ITIM_LIB` shared library on ISVI/WAS server and with ISIGADI include it in the jars of SDI running ISIGADI. With ISIQ, the handler is already included in the ISIQ side code. Required additions to the <ProtocollProperties> section of the `resource.def` when you are using ISIGADI and managing Top Secret profile assignments from both IBM Security Verify Governance Identity Manager and IBM Security Verify Governance.

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

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

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

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

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

Related concepts

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

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

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

Adapter profile installation verification

After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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.

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.

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

Adapter profile installation verification

After you install the adapter profile, verify that the installation is successful.

An unsuccessful installation might cause the following issues:

- Adapter functioning incorrectly.
- Prevents user from creating a service with the adapter profile.

To verify that the adapter profile is successfully installed, create a service with the adapter profile. For more information about creating a service, see “Creating an adapter service/target” on page xxvii.

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

Related concepts

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

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

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

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

Installing the adapter binaries or connector

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

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.

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries

The adapter requires access to the following jars at runtime.

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

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.

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.

Complete the “Importing the adapter profile” on page xxiii

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

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

1. Log on to the Identity server as an administrator.
2. In the **My Work** pane, click **Manage Services** > **Create**.
3. On the **Select the Type of Service** page, select IBM Security Verify Adapter for SCIM Adapter **Service**.
4. Click **Next** to display the adapter service form.
5. Complete the fields on the service form. See “Service Target/Form details” on page xxviii.

Related concepts

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

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details

This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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

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

Service Target/Form details

This tab provides general information about the adapter service.

Complete the service target/form details.

- "Service Information Tab" on page xxix
- "Dispatcher Attributes tab" on page xxx
- "Status and Information tab" on page xxxi

Related concepts

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

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

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

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

Service Information Tab

This tab provides information about the adapter service details.

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

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

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

IBM Security Directory Integrator location

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

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

IBM Security Verify Adapter for SCIM Adapter URL
Specify IBM Security Verify Adapter for SCIM Adapter URL of the IBM Security Verify Adapter for SCIM Adapter resource in this format: `https://<Instance- name>`. For example, `https://cloud.com/V2`.

Note: If the target system is integrated with Aquera, provide the SCIM Base URL generated by Aquera.

Authentication type
Specify the authentication type. Currently SCIM only supports OAuth. For example, OAuth.

Username
Specify the user name based on the authentication type and the target, if required.

Password
Specify the password based on the authentication type and the target, if required.

Bearer Token
Specify the bearer token based on the authentication type and the target, if required.

Note: If the target system is integrated with Aquera, provide the SCIM Base URL generated by Aquera.

SCIM Schema Extended File Path
Specify the SCIM Schema Extended File Path if target supports extended schema attributes. For example, `{SDI_HOME}/timsol/MappingFile/AttributeMapping.txt`.

Client ID
Specify the Client ID of API Client that is created with Administrator privileges. Obtain the Client ID from the **Configuration** > **API Access** -> from IBM Security Verify Adapter for SCIM Adapter.

Client Secret
Specify the client secret of the associated Client ID. Obtain the client secret from the **Configuration** > **API Access** tab from IBM Security Verify Adapter for SCIM Adapter.

Realm
Specify the realm name to manage the users from that realm through adapter.

Note: With this release of the adapter, this field is read-only and set to `cloudIdentityRealm`.

Proxy Host
Specify IP or hostname of Proxy Server.

Proxy Port
Specify Port number for Proxy Server.

Disable Email Notification
Select this check box to disable email notification while creating or modifying the user account.

Dispatcher Attributes tab

This tab describes the Dispatcher attributes.

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

- Assembly Line File System path
- Max connection count

Assembly Line File System Path

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

For example:

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

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

Disable Assembly Line Caching

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

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

Creating a new connection to the IBM Security Verify Adapter for SCIM Adapter resource can take a lot of time. Caching data can save time and resource utilization.

Max Connection Count

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

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

Assembly lines occupy the JVM memory. Too many assembly lines can cause an out-of-memory scenario in the IBM Security Directory Integrator server. Each assembly line also creates multiple

connections to the end point. The end point might have a limit on the number of remote connections allowed. As such, the adapter requests might fail.

Status and Information tab

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

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

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

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

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

Profile version
Specifies the version of the profile that is installed in the IBM Security Verify Governance Identity Manager.

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

Dispatcher version
Specifies the version of the Dispatcher.

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

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

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

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

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

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

Restarting the adapter service

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

Adapter profile installation verification
After you install the adapter profile, verify that the installation is successful.

Service Target/Form details
This tab provides general information about the adapter service.

Related tasks

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

Installing third-party client libraries
The adapter requires access to the following jars at runtime.

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

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.

Configuring

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

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

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

Suppressing password in clear text

While you are executing the user add and password change operations, the REST API shows the password in clear text.

To suppress the password in clear text, perform the following steps:

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.

Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Related concepts

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

Error messages and problem solving

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

Table 3 on page xxxvii and Table 4 on page xxxvii contain warnings or errors, which might be displayed when the IBM Security Verify Adapter for SCIM Adapter is installed on your system.

Table 3. Specific messages and actions

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

Table 4. 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 Identity Manager to refresh the list of attribute names.

Related concepts

Techniques for troubleshooting problems

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

Uninstalling

To remove an adapter from the Identity server for any reason, you must remove all the components that were added during installation. Uninstalling an IBM Security Directory Integrator-based adapter mainly involves removing the connector file and the adapter profile from the Identity server. Depending on the adapter, some of these tasks might not be applicable, or there can be other tasks.

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

Deleting the adapter profile

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

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

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

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

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

Reference

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

Adapter attributes

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

The IBM Security Verify Adapter for SCIM Adapter supports a standard set of attributes for user information.

The mandatory attributes to create an account are in the following table:

Table 5. Supported Account attributes

IBM Security Verify Adapter for SCIM Adapter attribute name	Description	Required
eruid	Username	YES
erscimGivenName	Given Name	YES
erscimSurName	Surname	YES
erscimDisplayName	Display Name	NO
erscimEmailWork	Work Email	YES
erscimEmailHome	Home Email	NO
erscimformattedname	Formatted Name	NO
erscimmiddlename	Middle Name	NO
erscimdisplayname	Display Name	NO
erscimworkphonenumber	Work Phone Number	NO
erscimMobilePhoneNumber	Mobile Number	NO
erscimstreet	Street	NO
erscimcity	City	NO
erscimaddress	Address	NO
erscimpostalcode	Postal Code	NO
erscimcountry	Country	NO
erscimregion	Region	NO
erscimjobtitle	Job Title	NO
erscimdepartment	Department	NO
erscimemployeeid	Employee ID	NO
erscimorganization	Organization	NO
erscimcostcenter	Cost Center	NO
erscimdivision	Division	NO

Table 5. Supported Account attributes (continued)		
IBM Security Verify Adapter for SCIM Adapter attribute name	**Description**	**Required**
erscimmanager	Manager	NO

Supported Group Attributes

Table 6. Supported Group Attributes		
IBM Security Verify Adapter for SCIM Adapter attribute name	**Description**	**Required**
erscimGroupID	Group ID	NO
erscimGroupName	Group Name	YES

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.

System Login Add

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

Table 7. Add request	
Required attribute	**Optional attribute**
erUid	All other supported attributes
erscimGivenName	
erscimSurName	
erscimEmailWork	

System Login Change

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

Table 8. Change request attribute	
Required attribute	**Optional attribute**
eruid	All other supported attributes

System Login Suspend

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

Table 9. Suspend request attributes	
Required attribute	**Optional attribute**
eruid	None
erAccountStatus	

System Login Restore

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

Table 10. Restore request attributes	
Required attribute	**Optional attribute**
eruid	None
erAccountStatus	

System Change Password

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

Table 11. System change password attributes	
Required attribute	**Optional attribute**
eruid	None
erPassword	

Test

The following table identifies attributes needed to test the connection.

Table 12. Test attributes	
Required attribute	**Optional attribute**
erscimbaseUrl	
erClientID	
erServicePwd1	
erauthtype	

Reconciliation

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

Table 13. Reconciliation request attributes	
Required attribute	**Optional attribute**
None	All other supported attributes

Adapter Configuration Properties

For information about setting IBM Security Directory Integrator configuration properties for the operation of the IBM Security Verify Adapter for SCIM Adapter, see the *Dispatcher Installation and Configuration Guide*.

Index