

IBM Security Verify Identity IBM Security
Verify Governance Identity Manager IBM
Security Privileged Identity Manager

*IBM Security Verify adapter Installation
and Configuration Guide*



Contents

- Figures..... V**
- Tables..... vii**
- Chapter 1. Overview..... 1**
 - Features of the adapter.....1
 - Architecture.....1
 - Supported configurations..... 1
- Chapter 2. Planning..... 3**
 - Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 6.x.... 3
 - Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x.... 5
 - Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager..... 7
 - Prerequisites..... 8
 - Software downloads..... 9
 - Software downloads..... 10
 - Installation worksheet..... 11
- Chapter 3. Installing..... 13**
 - Installing the dispatcher.....13
 - Installing the adapter binaries or connector.....14
 - Installing third-party client libraries..... 16
 - Configuring the SSL connection between the IBM Security Directory Integrator and the IBM Security Verify server.....17
 - Verifying the adapter installation..... 19
 - Restarting the adapter service..... 21
 - Importing the adapter profile..... 22
 - Importing the adapter profile..... 24
 - Importing the adapter profile..... 26
 - Importing attribute mapping file..... 28
 - Adding a connector..... 30
 - Enabling connectors..... 32
 - Reviewing and setting channel modes for each new connector..... 34
 - Attribute Mapping..... 36
 - Adapter profile installation verification..... 38
 - Creating an adapter service/target.....40
 - Service Target/Form details.....41
 - Service Information Tab..... 43
 - Dispatcher Attributes tab..... 43
 - Status and Information tab..... 44
 - Verifying that the adapter is working correctly..... 45
- Chapter 4. Upgrading.....47**
 - Upgrading the Dispatcher..... 47
 - Upgrading the adapter profile..... 47
- Chapter 5. Configuring..... 49**
 - Customizing the adapter profile..... 49

Preparing an MS-DOS ASCII file on the UNIX or Linux operating system.....	50
Suppressing password in clear text.....	51
Chapter 6. Troubleshooting.....	53
Techniques for troubleshooting problems.....	53
Error messages and problem solving.....	54
Chapter 7. Uninstalling.....	57
Deleting the adapter profile.....	57
Chapter 8. Reference.....	59
Required Accesses for API Client.....	59
Adapter attributes.....	59
Index.....	63

Figures

- 1. The architecture of the IBM Security Verify adapter..... 1
- 2. Example of a single server configuration..... 2
- 3. Example of a multiple server configuration..... 2

Tables

- 1. Preinstallation roadmap..... 3
- 2. Installation and configuration roadmap..... 3
- 3. Prerequisites to install the adapter.....9
- 4. Required information to install the adapter..... 11
- 5. Prerequisites for enabling a connector.....32
- 6. Specific messages and actions..... 55
- 7. General messages and actions..... 55
- 8. Supported Account attributes.....60
- 9. Supported Group Attributes.....60
- 10. Supported object classes.....60
- 11. Add request..... 61
- 12. Change request attribute..... 61
- 13. Suspend request attributes..... 61
- 14. Restore request attributes..... 61
- 15. System change password request attributes..... 61
- 16. Test attributes..... 62
- 17. Reconciliation request attributes..... 62

Chapter 1. Overview

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

IBM® Security Verify 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 Identity 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 server and IBM Security Verify Identity 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
- IBM Security Verify Adapter profile

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

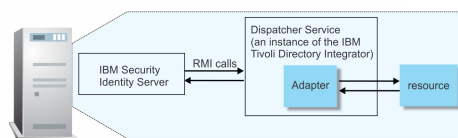


Figure 1. The architecture of the IBM Security Verify adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

- The Identity server
- The IBM Security Directory Integrator server

- The managed resource
- The adapter

The adapter must 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 server:

- Identity server
- Security Directory Integrator server
- IBM Security Verify adapter

The IBM Security Verify 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
- IBM Security Verify adapter
- IBM Security Verify server

The Security Directory Integrator server and the IBM Security Verify adapter are installed on the same server as shown in [Figure 3 on page 2](#).

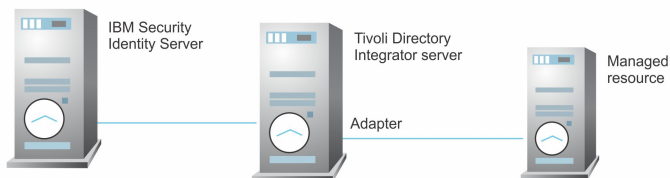


Figure 3. Example of a multiple server configuration

Chapter 2. Planning

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

Use the Preinstallation roadmap to prepare the environment.

Task	For more information, see
Verify that your environment meets the software and hardware requirements for the adapter.	“Prerequisites” on page 8.
Obtain the installation software.	“Software downloads” on page 10.
Obtain the necessary information for the installation and configuration.	“Installation worksheet” on page 11.

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

Task	For more information, see
Install the dispatcher.	Installing the dispatcher.
Install the connector.	“Installing the adapter binaries or connector” on page 14
Load the PeopleTools project in the IBM Security Verify Identity Governance Identity Manager IBM Security Privileged Identity Manager.	Loading the project
Import the adapter profile into the Identity server.	Importing the adapter profile
Create an adapter service.	Creating an adapter service
Configure the adapter.	Chapter 5, “Configuring,” on page 49

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

- Adapter attributes and object classes

- Adapter attributes by operations
- Special attributes

Related concepts

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

[Prerequisites](#)

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

[Software downloads](#)

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

[Software downloads](#)

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

[Installation worksheet](#)

The installation worksheet lists the information that is required to install and configure the adapter.

Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Related concepts

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 6.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

Prerequisites

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

Software downloads

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

Software downloads

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

Installation worksheet

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

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

3. Configure the adapter.
4. Modify the adapter profiles.
5. Customize the adapter.

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Related concepts

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 6.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[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.

[Software downloads](#)

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

[Installation worksheet](#)

The installation worksheet lists the information that is required to install and configure the adapter.

Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Prerequisites

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

[Table 3 on page 9](#) identifies the prerequisites for the adapter installation.

Table 3. Prerequisites to install the adapter

Prerequisite	Description
Directory Integrator	<ul style="list-style-type: none"> • IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 + FP4
Identity server	<p>The following servers are supported:</p> <ul style="list-style-type: none"> • IBM Security Identity Governance and Intelligence Server Version 5.2.5 • IBM Security Verify Identity v6.0 • IBM Security Verify Identity v7.0
IBM Security Verify server	IBM Security Verify server
IBM Security Directory Integrator adapters solution directory	A IBM Security Directory Integrator working directory for adapters. For more information, see, the <i>Dispatcher Installation and Configuration Guide</i> .
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 Identity 6.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

Software downloads

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

Software downloads

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

Installation worksheet

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

Software downloads

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

Go to [IBM Passport Advantage](#).

See the corresponding *IBM Security Verify Identity*, *IBM Security Verify Governance Identity Manager*, *IBM Security Privileged 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 Identity 6.x](#)

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

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

[Prerequisites](#)

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

[Software downloads](#)

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

[Installation worksheet](#)

The installation worksheet lists the information that is required to install and configure the adapter.

Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Software downloads

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

Go to [IBM Passport Advantage](#). See the *IBM Security Verify Governance Identity Manager Download Document*.

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

Related concepts

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 6.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

[Prerequisites](#)

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

[Software downloads](#)

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

[Installation worksheet](#)

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

Installation worksheet

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

Table 4. Required information to install the adapter		
Required information	Description	Value
IBM Security Directory Integrator Home Directory	The <i>ITDI_HOME</i> directory contains the <i>jars/connectors</i> subdirectory, which contains the files for the adapters.	Windows: <i>drive</i> \Program Files\IBM\TDI\V7.2 UNIX: <i>/opt/IBM/TDI/V7.2</i>
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 <i>Dispatcher Installation and Configuration Guide</i> .	Windows: <i>drive</i> \Program Files\IBM\TDI\V7.2\ UNIX: <i>/opt/IBM/TDI/V7.2/</i>
Create an API Client with a Client ID and a Client Secret on the IBM Security Verify resource	An API Client must to be created with the required administrator access for provisioning and managing the user accounts on IBM Security Verify server. Click Configuration > API Access tab on the resource with client ID and Client secret to create an API client. See “ Required Accesses for API Client ” on page 59.	

Related concepts

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 6.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x](#)
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

Prerequisites

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

Software downloads

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

Software downloads

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

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.

All IBM Security Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See [Installing the dispatcher](#).

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

Installing the dispatcher

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

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

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

Related concepts

[Verifying the adapter installation](#)

If the adapter is installed correctly, the `CloudIDConnector.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 IBM Security Verify server](#)

To enable SSL connection between the adapter and the IBM Security Verify 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.

[Importing the adapter profile](#)

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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 the adapter binaries or connector

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

Before you begin

The Dispatcher must be installed..

Procedure

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `CloudIDConnector.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 `CloudIDConnector.jar` file exists in the specified directory.

Restarting the adapter service

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

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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity, IBM Security Verify Governance Identity Manager, IBM Security Privileged Identity Manager account 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 third-party client libraries

The adapter requires access to the following jars at runtime.

Before you begin

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/>.

Procedure

1. Download the above-mentioned JAR files. Copy these files into `ITDI_HOME\jars\3rdparty\others` directory.
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 `CloudIDConnector.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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Configuring the SSL connection between the IBM Security Directory Integrator and the IBM Security Verify server

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

About this task

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

Procedure

1. On a web browser, go to your IBM Security Verify Instance URL. For example, `https://<IBM Security Verify instance url>/ui/admin`.
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 **Entrust (2048) certificate**.
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 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 cloudID -file c:\CloudID_cert.cer -keystore truststore.jks -storepass passwd
```

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=passwd`
 - `javax.net.ssl.trustStoreType=jks`

If these key properties are not configured, you can set truststore to the same that contains the IBM Security Verify server certificate. Otherwise, you must import the IBM Security Verify server 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 `CloudIDConnector.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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity Manager account 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.

Verifying the adapter installation

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

Windows operating system

`drive:\Program Files\IBM\TDI\7.1\jars\connectors\`

UNIX operating system

`/opt/IBM/TDI/7.1/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 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 tasks 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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity Manager, IBM Security Verify Governance Identity Manager, IBM Security Privileged Identity Manager account 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.

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 `CloudIDConnector.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 IBM Security Verify server](#)

To enable SSL connection between the adapter and the IBM Security Verify 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.

[Importing the adapter profile](#)

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

[Importing the adapter profile](#)

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

[Importing attribute mapping file](#)

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity Manager account 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.

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System > Manage Service Types**.
The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.
The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:

- a) In the **Service Definition File** field, type the directory location of the <Adapter>Profile.jar file, or click **Browse** to locate the file.
For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the ADProfileJAR file.
- b) Click **OK** to import the file.

Results

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

What to do next

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

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.

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

Results

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

What to do next

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

Related concepts

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 `CloudIDConnector.jar` file exists in the specified directory.

Restarting the adapter service

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

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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Importing the adapter profile

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

Before you begin

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

About this task

Target definition files are also called adapter profile files.

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

Procedure

1. On the Appliance Dashboard, select Verify Governance Identity Manager Administration Console from the **Quick Links** widget.
The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**.
The Target Administration console is displayed.
3. From the navigation tree, select **Manage Target Types**.
The **Manage Target Types** page is displayed.
4. On the **Manage Target Types** page, click **Import**.
The **Import Target Type** page is displayed.
5. On the **Import Target Type** page, complete these steps:
 - a) In the **Target Definition File** field, click **Browse** to locate the `<Adapter>Profile.jar` file.
For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the ADProfileJAR file.
 - b) Click **OK**.
A message indicates that you successfully imported a target type.
6. Click **Close**.

What to do next

- The import occurs asynchronously, which means it might take some time for the target type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Target Types** page, click **Refresh** to see the new target type. If the target type is not displayed in a reasonable amount of time, 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. On the Appliance Dashboard, select **Manage System Settings > Maintenance > Log Retrieval and Configuration > Identity > trace log**, then click **View**.

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 `CloudIDConnector.jar` file exists in the specified directory.

Restarting the adapter service

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

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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager account 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.

Importing attribute mapping file

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

About this task

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

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage > Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions > Import**.
6. On the **Import** page, complete these steps:
 - a) Select **Attribute Mapping**.

b) Click **Browse** to locate the attribute mapping file that you want to import.

c) Click **Upload file**.

A message indicates that you successfully imported the file.

7. Click **Close**.

Related concepts

Installing the dispatcher

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

Verifying the adapter installation

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

Restarting the adapter service

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

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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Adding a connector

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

Before you begin

Complete [Importing the adapter profile](#).

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

About this task

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

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

Procedure

To add a connector, complete these steps.

1. Log in to the Verify Governance Identity Manager Administration Console.
 2. From the Administration Console, select **Enterprise Connectors**.
 3. Select **Manage > Connectors**.
- A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
 5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
 6. Click **Actions > Add**.

The **Connector Details** pane is enabled for your input.

7. On the **Connector Details** tab, complete these steps:
 - a) Assign a name and description for the connector.
 - b) Select the target profile type as **Identity Brokerage** and its corresponding target profile.
 - c) Select the entity, such as **Account** or **User**.

Depending on the connector type, this field might be preselected.
 - d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.

The available trace levels are DEBUG, INFO, and ERROR.
 - e) Optional: Select **History ON** to save and track the connector usage.
 - f) Click **Save**.

The fields for enabling the channels for sending and receiving data are now visible.
 - g) Select and set the connector properties in the **Global Config** accordion pane.

For information about the global configuration properties, see [Global Config accordion pane](#).

h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

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

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

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see [“Enabling connectors” on page 32](#).

Related concepts

[Installing the dispatcher](#)

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

[Verifying the adapter installation](#)

If the adapter is installed correctly, the `CloudIDConnector.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 IBM Security Verify server](#)

To enable SSL connection between the adapter and the IBM Security Verify 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.

[Importing the adapter profile](#)

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

[Importing the adapter profile](#)

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

[Importing attribute mapping file](#)

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

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 IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Enabling connectors

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

Before you begin

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

Procedure

To enable a connector, complete these steps:

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

Enable write-to channel

Propagates every change in the Access Governance Core repository into the target system.

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

Enable read-from channel

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

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

Enable reconciliation

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

Results

The connector is enabled

What to do next

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

Related conceptsInstalling 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 `CloudIDConnector.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 tasksInstalling 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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

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 IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Reviewing and setting channel modes for each new connector

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

About this task

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

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

Procedure

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

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

Enable write-to channel

Propagates every change in the Access Governance Core repository into the target system.

Enable read-from channel

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

Enable reconciliation

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

8. Select **Monitor > Change Log Sync Status**.

A list of connectors is displayed.

9. On the **Change Log Sync Status** tab, complete these steps:

- a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
- b) Select a connector, and click **Actions > Sync Now**.
The synchronization process begins.
- c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane. Information about the synchronization is displayed in the **Sync History** tab.

10. Set the change log synchronization schedule for each new connector that you migrated.

11. When the connector configuration is complete, enable the connector by completing these steps:

- a) Select **Manage > Connectors**.
- b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
- c) Click **Save**.

For more information, see [“Enabling connectors” on page 32](#).

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

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

12. Start the connector by selecting **Monitor > Connector Status**. Select the connector that you want to start, and then select **Actions > Start**.

Related concepts

Installing the dispatcher

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

Verifying the adapter installation

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

Restarting the adapter service

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

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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account attributes.

About this task

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

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

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

Some <IGI_attribute> do not have a defined <target_attribute> and you can assign the mapping. For example, surName=surName and ATTR1=ATTR1.

Note:

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

Procedure

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

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

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

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

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see Attribute-to-permission mapping service in the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager product documentation.
6. Map the following attributes for Channel-Write To and Channel-Read From.

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

Related concepts

Installing the dispatcher

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

Verifying the adapter installation

If the adapter is installed correctly, the CloudIDConnector.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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

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 40](#).

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 `CloudIDConnector.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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Creating an adapter service/target

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

Before you begin

Complete the [“Importing the adapter profile”](#) on page 22 [“Importing the adapter profile”](#) on page 24

About this task

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

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

Procedure

1. 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 **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 41.

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 `CloudIDConnector.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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account attributes.

Verifying that the adapter is working correctly

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

Service Target/Form details

This tab provides general information about the adapter service.

Complete the service target/form details.

- [“Service Information Tab” on page 43](#)
- [“Dispatcher Attributes tab” on page 43](#)
- [“Status and Information tab” on page 44](#)

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 `CloudIDConnector.jar` file exists in the specified directory.

Restarting the adapter service

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

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 IBM Security Verify server

To enable SSL connection between the adapter and the IBM Security Verify 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.

Importing the adapter profile

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

Importing the adapter profile

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

Importing attribute mapping file

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

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 Identity 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 URL

Specify IBM Security Verify URL of the IBM Security Verify resource in this format: `https://<Instance-name>`. For example, `https://adapters.ice.ibmcloud.com`.

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.

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.

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.

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 Identity IBM Security Verify Governance Identity Manager IBM Security Privileged 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 resource is maintained. The next request that the adapter receives can reuse this connection.

Creating a new connection to the IBM Security Verify 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 Identity.

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.

Procedure

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

Related concepts

[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 `CloudIDConnector.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 IBM Security Verify server](#)

To enable SSL connection between the adapter and the IBM Security Verify 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.

[Importing the adapter profile](#)

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

[Importing the adapter profile](#)

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

[Importing attribute mapping file](#)

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

Adding a connector

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

Enabling connectors

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

Reviewing and setting channel modes for each new connector

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

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager account 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.

Chapter 4. Upgrading

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

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

Upgrading the Dispatcher

The new adapter package might require an upgrade of the Dispatcher.

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

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

Note: Stop the Dispatcher service before the upgrade and restarts it after the upgrade is complete.

Related concepts

[Upgrading the adapter profile](#)

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

Upgrading the adapter profile

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

Note: Restart the Dispatcher service after importing the profile. Restarting the Dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.

Related concepts

[Upgrading the Dispatcher](#)

The new adapter package might require an upgrade of the Dispatcher.

Chapter 5. Configuring

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

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

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

Customizing the adapter profile

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

About this task

Use the Form Designer or the `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file.

The JAR file is included in the adapter package that you downloaded from the IBM Passport Advantage website. The JAR file and the files in the JAR file vary depending on your operating system.

The adapter profile JAR file includes the following files:

- `erTDICloudIDAccount.xml`
- `erTDICloudIDRMIService.xml`
- `TDICloudIDTest.xml`
- `CloudIDAdd.xml`
- `CloudIDSearch.xml`
- `CloudIDModify.xml`
- `CloudIDDelete.xml`
- `targetProfile.json`
- `schema.dsm1`
- `service.def`

Procedure

1. Edit the JAR file.
 - a) Log on to the workstation where the IBM Security Verify adapter is installed.
 - b) On the **Start** menu, select **Programs → Accessories → Command Prompt**.
 - c) Copy the JAR file into a temporary directory.
 - d) Extract the contents of the JAR file into the temporary directory by running the following command.
Type the name of the JAR file for your operating system.

The following example applies to the IBM Security Verify adapter profile.

```
cd c:\temp cd /tmp
jar -xvf CloudIDAdapterProfile.jar
```

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

- e) Edit the file that you want to change.

After you edit the file, you must import the file into the Identity server for the changes to take effect.

2. Import the file.

- a) Create a JAR file by using the files in the directory.

Run the following commands:

Windows

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

UNIX

```
cd /tmp
jar -cvf CloudIDAdapterProfile.jar CloudIDAdapterProfile
```

- b) Import the JAR file into the IBM Security Verify IdentityIBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity ManagerIBM Security Privileged Identity Manager application server.
- c) Stop and start the Identity server
- d) Restart the adapter service.

Related concepts

[Preparing an MS-DOS ASCII file on the UNIX or Linux operating system](#)

The adapter profile .jar file might contain ASCII files in MS-DOS ASCII format.

Related tasks

[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.

Preparing an MS-DOS ASCII file on the UNIX or Linux operating system

The adapter profile .jar file might contain ASCII files in MS-DOS ASCII format.

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

You can use the **vi** editor to remove the ^M characters manually. From the **vi** command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter ^M or Ctrl-M by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as a command.

Related tasks

[Customizing the adapter profile](#)

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

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.

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.

About this task

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

Procedure

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

Preparing an MS-DOS ASCII file on the UNIX or Linux operating system

The adapter profile .jar file might contain ASCII files in MS-DOS ASCII format.

Related tasks

Customizing the adapter profile

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

Chapter 6. Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Related concepts

[Error messages and problem solving](#)

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

Error messages and problem solving

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

[Table 6 on page 55](#) and [Table 7 on page 55](#) contain warnings or errors, which might be displayed when the IBM Security Verify adapter is installed on your system.

Table 6. Specific messages and actions

Message number	Message	Action
CTGIMT600E	An error occurred while establishing communication with the IBM Security Directory Integrator server.	<ul style="list-style-type: none"> • 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 URL is correct	<ul style="list-style-type: none"> • Verify that the IBM Security Verify server URL is running. • Verify that the IBM Security Verify client ID and client secret that is specified on the service form of the IBM Security Verify server are correct.
CTGIMU107W	The following error occurred: 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 7. 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 <i>ITDI_HOME</i> /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 Identity IBM Security Verify Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager IBM Security Privileged Identity Manager to refresh the list of attribute names.

Related concepts

Techniques for troubleshooting problems

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

Chapter 7. Uninstalling

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

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 Identity IBM Security Verify Governance Identity Manager IBM Security Privileged Identity Manager product documentation.

Chapter 8. Reference

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

Required Accesses for API Client

An API Client must be created with the required administrative accesses for provisioning and managing the user accounts on the IBM Security Verify server. The API Client is created under **Configuration > API Access > tab on resource with client ID and client secret.**

The following list is a list of accesses that are required to be granted to the API client on the IBM Security Verify resource:

- Authenticate any user
- Manage access policies
- Manage API clients
- Manage application entitlements
- Manage application lifecycle
- Manage authenticator configuration
- Manage authenticator registrations for all users
- Manage OIDC and OAuth grants
- Manage password policy
- Manage push notification credentials
- Manage second-factor authentication enrollment for all users
- Manage second-factor authentication method configuration
- Manage templates
- Manage users, standard groups, and reserved groups
- Read authenticator configuration
- Read authenticator registrations for all users
- Read OIDC and OAuth grants
- Read password policy
- Read push notification credentials
- Read second-factor authentication enrolment for all users
- Read second-factor authentication method configuration
- Read templates
- Read users and groups
- Recover username
- Reset password

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 supports a standard set of attributes for user information.

The mandatory attributes to create an account are:

- User Name
- Given Name
- Surname
- Email

<i>Table 8. Supported Account attributes</i>		
IBM Security Verify adapter attribute name	Description	Required
eruid	Username	YES
erCloudIdentityGivenName	Given Name	YES
erCloudIdentitySurName	Surname	YES
erCloudIdentityDisplayName	Display Name	NO
erCloudIdentityEmail	Email	YES
erCloudIdentityMobilePhoneNumber	Mobile Number	NO
erCloudIdentityRealm	Realm	NO
erCloudIdentityGroupMember	Groups	NO

Supported Group Attributes

<i>Table 9. Supported Group Attributes</i>		
IBM Security Verify adapter attribute name	Description	Required
erCloudIdentityGroupID	Group ID	NO
erCloudIdentityGroupName	Group Name	YES
erCloudIdentityGroupType	Group Type	NO

Object Classes

<i>Table 10. Supported object classes</i>	
Description	Object class name in schema
Service class	erTDICloudIDRMIService
Account class	erTDICloudIDAccount
Group class	erTDICloudIdentityGroup

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.

<i>Table 11. Add request</i>	
Required attribute	Optional attribute
erUid	All other supported attributes
erCloudIdentityGivenName	
erCloudIdentitySurName	
erCloudIdentityEmail	

System Login Change

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

<i>Table 12. Change request attribute</i>	
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.

<i>Table 13. Suspend request attributes</i>	
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.

<i>Table 14. Restore request attributes</i>	
Required attribute	Optional attribute
eruid	None
erAccountStatus	

System Change Password

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

<i>Table 15. System change password request attributes</i>	
Required attribute	Optional attribute
eruid	None
erPassword	

Test

The following table identifies attributes needed to test the connection.

<i>Table 16. Test attributes</i>	
Required attribute	Optional attribute
erCloudIdentityUrl	erCloudIdentityProxyHost erCloudIdentityProxyPort
erCIClientID	
erServicePwd1	
erCloudIdentityRealm	

Reconciliation

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

<i>Table 17. Reconciliation request attributes</i>	
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, see the *Dispatcher Installation and Configuration Guide*.

Index

A

- account
 - management automation [1](#)
- adapter
 - account management automation [1](#)
 - attributes [59](#)
 - customization steps [49](#)
 - features [1](#)
 - installation
 - home directory [11](#)
 - solution directory [11](#)
 - troubleshooting errors [53](#)
 - verifying [45](#)
 - warnings [53](#)
 - worksheet [11](#)
 - profile
 - removal [57](#)
 - supported configurations
 - multiple server [1](#)
 - single server [1](#)
 - uninstallation [57](#)
 - upgrade [47](#)
- attributes
 - mandatory [59](#)
 - standard [59](#)
- automation, account management [1](#)

D

- dispatcher
 - installation [13](#)
- download, software [9](#), [10](#)

E

- error messages [54](#)

I

- installation
 - first steps after
 - adapter configuration [49](#)
 - adapter verification [49](#)
 - language pack installation [49](#)
 - SSL setup [49](#)
 - planning roadmaps [3](#)
 - verification
 - adapter [45](#)
 - worksheet
 - home directory [11](#)
 - solution directory [11](#)

M

- messages

- messages (*continued*)
 - error [54](#)
 - warning [54](#)
- MS-DOS ASCII characters [50](#)

O

- operating system prerequisites [8](#)

P

- post-installation steps
 - adapter configuration [49](#)
 - adapter verification [49](#)
 - language pack installation [49](#)
 - SSL setup [49](#)
- profile
 - editing on UNIX or Linux [50](#)
 - removal [57](#)

R

- roadmaps
 - planning [3](#)

S

- software
 - download [9](#), [10](#)
 - requirements [8](#)
 - website [9](#), [10](#)
- supported configurations
 - adapter
 - multiple server [1](#)
 - single server [1](#)
 - overview
 - multiple server [1](#)
 - single server [1](#)

T

- troubleshooting
 - error messages [54](#)
 - identifying problems [53](#)
 - techniques for [53](#)
 - warning messages [54](#)
- troubleshooting and support
 - troubleshooting techniques [53](#)

U

- uninstallation
 - adapter [57](#)
 - advance notice to users [57](#)
- updating
 - adapter profile [49](#)

V

- verification
 - dispatcher installation [13](#)
 - installation [45](#)
 - software
 - prerequisites [8](#)
 - requirements [8](#)
 - system prerequisites [8](#)
 - system requirements [8](#)
- vi command [50](#)

W

- warning messages [54](#)

