IBM Security Verify Governance Identity Manager

IBM Security Verify Governance Identity Manager Admin Realm Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

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

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

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

Features of the adapter

The adapter automates several administrative and management tasks.

The adapter supports the following tasks:

- Reconciling user accounts and support data
- Adding and modifying user accounts
- Modifying user account attributes
- Modifying user account password
- Suspending and restoring user accounts
- Deleting user accounts

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 Governance Identity Manager

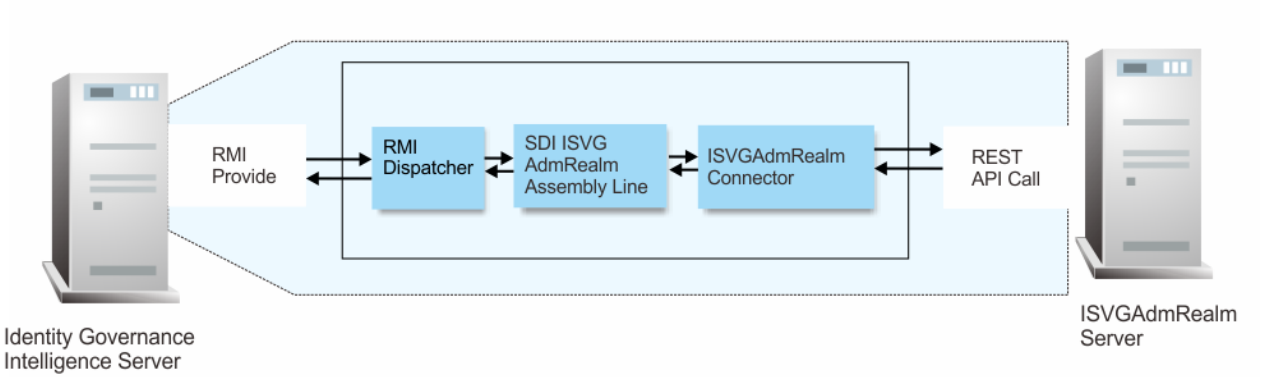

Figure 1. The architecture of the IBM Security Verify adapter

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.

Prerequisites

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

Table 1 on page 3 identifies the prerequisites for the adapter installation.

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Directory Integrator	IBM Security Directory Integrator Version 7.6 + FP4 + 7.2.0-ISS-SDI-LA0019
IBM Security Verify Governance Identity Manager	Identity server
IBM Security Verify Governance Identity Manager Admin Realm	IBM Security Verify Governance Identity Manager Admin Realm version 5.2.6
IBM Security Directory Integrator adapters solution directory	A IBM Security Directory Integrator working directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*.
System administrator authority	You must have system administrator authority to complete the adapter installation procedure.

Related concepts

Installation worksheet

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

Installation worksheet

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

Table 2. Required information to install the adapter

Required information	Description	Value
IBM Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory, which contains the files for the adapters.	**Windows:** *drive*`\Program Files\IBM\TDI\V7.2` **UNIX:** `/opt/IBM/TDI/V7.2`

Table 2. Required information to install the adapter (continued)		
Required information	**Description**	**Value**
Adapter Solution Directory	When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. For more information, see the *Dispatcher Installation and Configuration Guide*.	**Windows:** *drive*\Program Files\IBM\TDI\V7.2\ **UNIX:** /opt/IBM/TDI/V7.2/

Related concepts

Prerequisites

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

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 `ISVGAdmRealm.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
Perform the following steps to install the adapter.

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

Enabling TLSv1.2 in Security Directory Integrator

Configuring the SSL connection between the IBM Security Directory Integrator and the Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

Installing the adapter

Perform the following steps to install the adapter.

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

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

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

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

Related tasks

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

Enabling TLSv1.2 in Security Directory Integrator

Configuring the SSL connection between the IBM Security Directory Integrator and the Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

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:

- `commons-logging-1.2.jar`

  Download the commons-logging-1.2.jar from https://mvnrepository.com/artifact/commons-logging/commons-logging/1.2
- `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/.
- `commons-codec-1.9.jar`

Download the commons-codec-1.9.jar from https://mvnrepository.com/artifact/commons-codec/commons-codec/1.9

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 `ISVGAdmRealm.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
Perform the following steps to install the adapter.

Enabling TLSv1.2 in Security Directory Integrator

Configuring the SSL connection between the IBM Security Directory Integrator and the Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

Enabling TLSv1.2 in Security Directory Integrator

About this task

Procedure

1. Apply recommended fix packs and limited availability (LA) versions on the Security Directory Integrator. See Recommended fixes for IBM Tivoli Directory Integrator (TDI) & IBM Security Directory Integrator (SDI).
2. After applying the appropriate updates, modify the <SOLUTION_DIRECTORY>/`solution.properties` file by appending the following text to the bottom of the file:

```
##

# # Protocols to enforce SSL protocols in a SDI Server
# # Optional values for com.ibm.di.SSL* property (TLSv1, TLSv1.1, TLSv1.2). # # This can be
a multi-valued comma separated property
# # Optional values for com.ibm.jsse2.overrideDefaultProtocol property (SSL_TLSv2,
TLSv1,TLSv11,TLSv12).
# # This is a single value property.
```

```
##
-
com.ibm.di.SSLProtocols=TLSv1,TLSv1.1,TLSv1.2
com.ibm.di.SSLServerProtocols=TLSv1,TLSv1.1,TLSv1.2
com.ibm.jsse2.overrideDefaultProtocol=TLSv1 com.ibm.jsse2.overrideDefaultTLS=true
```

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 `ISVGAdmRealm.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
Perform the following steps to install the adapter.

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 Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

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

To enable SSL connection between the adapter and the Identity 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 Governance Identity Manager Instance URL. For example, `https://<{host}:{port}>/ideas/desk?realm=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. On a web browser, navigate to the IBM Security Verify Governance Identity Manager virtual appliance dashboard. For example, `https://<{host}:{port}>/dashboard`. Repeat steps “2” on page 8 to “5” on page 8.

7. Perform one of the following actions:
   - If the RMI Dispatcher already has a configured keystore, use the `keytool.exe` program to import the Identity 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 isvgAdminRealmId -file c:\isvg_realm.cert.cer -
     keystore truststore.jks -storepass passw0rd
     ```

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 `ISVGAdmRealm.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
Perform the following steps to install the adapter.

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

Enabling TLSv1.2 in Security Directory Integrator

Installing the MILT-Tags file

Installing the MILT-Tags file

About this task

Ensure that the Dispatcher is installed.

Procedure

Copy the files from **ILMT-Tags** folder to the specified location:

- Windows: `<SDI-HOME>/swidtag`
- Unix/Linux: `<SDI-HOME>/swidtag`

Related concepts

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

Verifying the adapter installation
If the adapter is installed correctly, the `ISVGAdmRealm.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
Perform the following steps to install the adapter.

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

Enabling TLSv1.2 in Security Directory Integrator

Configuring the SSL connection between the IBM Security Directory Integrator and the Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Verifying the adapter installation

If the adapter is installed correctly, the `ISVGAdmRealm.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/`

Related concepts

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

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

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

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

Related tasks

Installing the adapter
Perform the following steps to install the adapter.

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

Enabling TLSv1.2 in Security Directory Integrator

Configuring the SSL connection between the IBM Security Directory Integrator and the Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

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

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 `ISVGAdmRealm.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
Perform the following steps to install the adapter.

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

Enabling TLSv1.2 in Security Directory Integrator

Configuring the SSL connection between the IBM Security Directory Integrator and the Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

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.

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 `ISVGAdmRealm.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
Perform the following steps to install the adapter.

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

Enabling TLSv1.2 in Security Directory Integrator

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

To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

Service Target/Form details

This tab provides general information about the adapter service.

Complete the service target/form details.

- "Service Information Tab" on page 12
- "Dispatcher Attributes tab" on page 13
- "Status and Information tab" on page 13

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

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

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

Related tasks

Installing the adapter
Perform the following steps to install the adapter.

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

Enabling TLSv1.2 in Security Directory Integrator

Configuring the SSL connection between the IBM Security Directory Integrator and the Identity server
To enable SSL connection between the adapter and the Identity server, Configure the keystores for the Dispatcher.

Installing the MILT-Tags file

Service Information Tab

This tab provides information about the adapter service details.

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

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

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

IBM Security Directory Integrator location

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

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

ISVG Admin Realm API URL
Specify login URL of ISVG admin realm server. For example, `https://{host}:{port}/`

ISVG Admin Realm Username
Specify ISVG Admin realm user name.

ISVG Admin Realm Password
Specify ISVG Admin realm password.

Dispatcher Attributes tab

This tab describes the Dispatcher attributes.

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

- Assembly Line File System path
- Max connection count

Assembly Line File System Path

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

For example:

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

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

Disable Assembly Line Caching

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

Select the check box if the requirement is to enable caching. When enabled, the entire assembly line object is saved in the cache. The connection to the IBM Security Verify 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.

SDI 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.

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 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 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:

- `CustomLabels.xml`
- `erISVGAdmRealmAccount.xml`
- `erISVGAdmRealmService.xml`
- `ISVGAdmRealmTest.xml`
- `ISVGAdmRealmAdd.xml`
- `ISVGAdmRealmSearch.xml`
- `ISVGAdmRealmModify.xml`
- `ISVGAdmRealmDelete.xml`
- `targetProfile.json`
- `schema.dsml`
- `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 ISVGAdmRealmAdapterProfile.jar
```

The **jar** command extracts the files into the `ISVGAdmRealmAdapterProfile` 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 ISVGAdmRealmAdapterProfile.jar ISVGAdmRealmAdapterProfile
```

UNIX

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

b) Import the JAR file into the IBM Security Verify Governance Identity Manager application server.

c) Stop and start the Identity server

d) Restart the adapter service.

Editing adapter profiles 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.

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 3 on page 21 contain warnings or errors, which might be displayed when the IBM Security Verify adapter is installed on your system.

Table 3. Specific messages and actions

Message number	Message	Action
CTGIMT001E	The following error occurred. Error during authentication. Ensure Client ID, Client Secret, and the IBM Security Verify URL is correct	• Verify that the Identity server URL is running. • Verify that the IBM Security Verify client ID and client secret that is specified on the service form of the Identity server are correct.
CTGIMT002E	The login credential is missing or incorrect.	Verify that you provided correct login credential on service form
CTGIMT003E	The account already exists.	Use a different name for the user to be added.
CTGIMT004E	The adapter does not have permission to add an account: Account_Name	The administrator user that is provided on the IBM Security Directory Integrator service form does not have the required privileges to add a user account. Ensure that an administrator user with the required privileges is specified on service form. These privileges are the minimum that are required for the administrator user: **CREATEROLE** Create Role permission **SUPERUSER** Superuser administrator authority
CTGIMT600E	An error occurred while establishing communication with the IBM Security Directory Integrator server.	IBM Security Verify Governance Identity Manager cannot establish a connection with IBM Security Directory Integrator. To fix this problem, ensure that: • IBM Security Directory Integrator is running. • The URL specified on the service form for the IBM Security Directory Integrator is correct.
CTGIMT015E	An error occurred while deleting the Account Name because the account does not exist.	The user you trying to delete does not exist. Ensure that you are deleting only an existing account.

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 Governance 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.

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 Governance Identity Manager adapter supports a standard set of attributes for user information.

The mandatory attributes to create an account are:

- User Name
- OU Master

Table 4. Supported Account attributes

IBM Security Verify adapter attribute name	Description	Required
eruid	Username	YES
erisvgadmrealmoumaster	OU Master	YES
erisvgadmrealmsysuid	usesysid (ReadOnly)	NO
erisvgadmrealmusertype	User Type	NO
erisvgadmrealmmasteruid	loginName	NO
erisvgadmrealmaccountexp	Account Expiration	NO
erisvgadmrealmfirstname	First Name	NO
erisvgadmrealmlastname	Last Name	NO
erPassword	Password	NO
erisvgadmrealmemail	Email	NO
erisvgadmrealmphone	Phone Number	NO
erisvgadmrealmdn	DN	NO
erisvgadmrealmfiscode	SSN/Fiscal Code	NO
erisvgadmrealmgender	Gender	NO
erisvgadmrealmdob	Date of Birth	NO
erisvgadmrealmpob	Place of Birth	NO
erisvgadmrealmaddress	Addrss	NO
erisvgadmrealmcity	City	NO
erisvgadmrealmstate	State	NO
erisvgadmrealmcountry	Country	NO
erisvgadmrealmzip	Zip/Postal Code	NO
erisvgadmrealmidentityuid	Identity Uid (Read Only)	NO

Table 4. Supported Account attributes (continued)		
IBM Security Verify adapter attribute name	**Description**	**Required**
erisvgadmrealmmasteruid	Master Uid (Read Only)	NO

Supported Group Attributes

Table 5. Supported Group Attributes		
IBM Security Verify adapter attribute name	**Description**	**Required**
erISVGAdmRealmGroupID	Group ID	NO
erISVGAdmRealmGroupName	Group Name	NO
erISVGAdmRealmDes	Group Type	NO

Table 6. Supported Business Role External role Attributes		
IBM Security Verify Governance Identity Manager adapter attribute name	**Description**	**Required**
erISVGAdmRealmRoleId	Id	YES
erISVGAdmRealmRoleName	Name	YES
erISVGAdmRealmApplicationName	App Name	NO

Table 7. Supported IT Role External role Attributes		
IBM Security Verify Governance Identity Manager adapter attribute name	**Description**	**Required**
erISVGAdmRealmITRoleId	Id	YES
erISVGAdmRealmITApplicationName	App Name	NO
erISVGAdmRealmITRoleName	Name	YES

Table 8. Supported Permission Attributes		
IBM Security Verify Governance Identity Manager adapter attribute name	**Description**	**Required**
erISVGAdmRealmPermId	Id	YES
erISVGAdmRealmPermName	Name	YES
erISVGAdmRealmAppName	App Name	NO

Object Classes

Table 9. Supported object classes	
Description	**Object class name in schema**
Service class	**erISVGAdmRealmService**

Table 9. Supported object classes (continued)	
Description	**Object class name in schema**
Account class	**erISVGAdmRealmAccount**
Group class	**erISVGAdmRealmGroup**
Role class	**erISVGAdmRealmRole**
IT Role class	**erISVGAdmRealmITRole**
Permission class	**erISVGAdmRealmRolePerm**

Adapter attributes by operations

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

System Login Add

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

Table 10. Add request	
Required attribute	**Optional attribute**
eruid	All other supported attributes

System Login Change

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

Table 11. Change request attribute	
Required attribute	**Optional attribute**
eruid	All other supported attributes

System Login Suspend

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

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

System Login Restore

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

Table 12. Restore request attributes	
Required attribute	**Optional attribute**
eruid	None
erAccountStatus	

Test

The following table identifies attributes needed to test the connection.

Table 13. Test attributes	
Required attribute	**Optional attribute**
erisvgadmrealmurl	None
erisvgadmrealmapiuser	
erservicename	
erserviceuid	
erisvgadmrealmapikey	

Reconciliation

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

Table 14. Reconciliation request attributes	
Required attribute	**Optional attribute**
None	All other supported attributes

Index