IBM Security Verify Identity

IBM Security Secret Server and Thycotic Secret server 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 3
- Prerequisites 4
- Software downloads 5
- Installation worksheet 6

Chapter 3. Installing 7
- Installing the dispatcher 7
- Installing the adapter binaries or connector 8
- Installing third-party client libraries 9
- Configuring the SSL connection between the IBM Security Directory Integrator and the IBM Security Secret Server and Thycotic Secret server 10
- Verifying the adapter installation 11
- Restarting the adapter service 12
- Importing the adapter profile 13
- Adapter profile installation verification 15
- Creating an adapter service/target 16
- Service Target/Form details 17
  - Service Details 18
  - Connection Details tab 18
  - Dispatcher Attributes tab 18
  - Status and Information tab 19
- Verifying that the adapter is working correctly 20

Chapter 4. Upgrading 21
- Upgrading the Dispatcher 21
- Upgrading the adapter profile 21

Chapter 5. Configuring 23
- Customizing the adapter profile 23
- Preparing an MS-DOS ASCII file on the UNIX or Linux operating system 24

Chapter 6. Troubleshooting 25
- Techniques for troubleshooting problems 25
- Error messages and problem solving 26

Chapter 7. Uninstalling 29
- Deleting the adapter profile 29

Chapter 8. Reference..... 31
Adapter attributes.....31

Index..... 35

Figures

1. The architecture of the IBM Security Secret Server and Thycotic Secret server adapter.....1

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

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

Tables

1. Prerequisites to install the adapter....5

2. Required information to install the adapter....6

3. Specific messages and actions....27

4. General messages and actions....27

5. Supported Account attributes....31

6. Supported Group Attributes....31

7. Supported object classes....32

8. Add request....32

9. Change request attribute....32

10. Suspend request attributes....33

11. Restore request attributes....33

12. System change password request attributes....33

13. Test attributes....33

14. Reconciliation request attributes....33

Chapter 1. Overview

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

IBM® Security Verify Identity 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 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, Folders, and Secrets.
- 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 Secret Server and Thycotic Secret server and IBM Security Verify Identity 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.

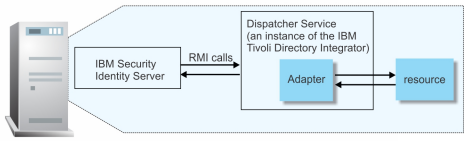

Figure 1. The architecture of the IBM Security Secret Server and Thycotic Secret server adapter

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 Secret Server and Thycotic Secret server:

- Identity server
- Security Directory Integrator server
- IBM Security Secret Server and Thycotic Secret server adapter

The IBM Security Secret Server and Thycotic Secret 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 Secret Server and Thycotic Secret server adapter
- IBM Security Secret Server and Thycotic Secret server

TheSecurity Directory Integrator server and the IBM Security Secret Server and Thycotic Secret server adapter are installed on the same server as shown in Figure 3 on page 2.

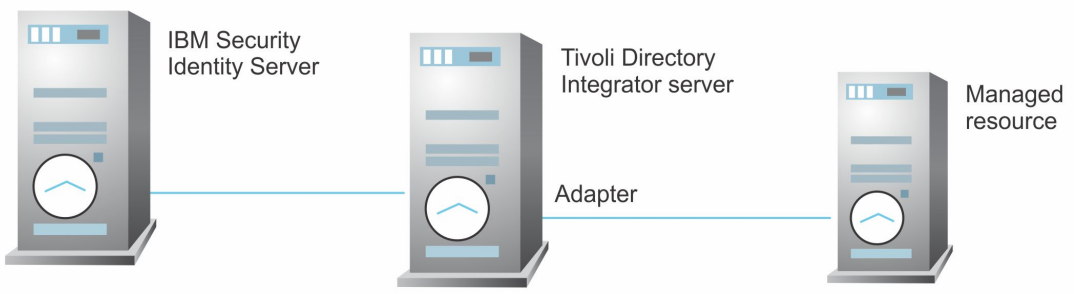

Figure 3. Example of a multiple server configuration

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.

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

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

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

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

Prerequisites

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

Table 1 on page 5 identifies the prerequisites for the adapter installation.

Table 1. Prerequisites to install the adapter	
Prerequisite	**Description**
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	The following servers are supported: • IBM Security Verify Identity v7.0
IBM Security Secret Server and Thycotic Secret server	Version 10.4 Enterprise Plus Edition
Security Directory Integrator adapters solution directory	A Security Directory Integrator work directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*.
System administrator authority	You must have system administrator authority to complete the adapter installation procedure.

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.

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

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

Software downloads

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

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Identity 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 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.

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
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`
Adapter Solution Directory	When you install the dispatcher, the installer prompts you to specify a filepath for the solution directory. For more information, see the *Dispatcher Installation and Configuration Guide*.	**Windows:** *drive*`\Program Files\IBM\TDI\V7.2\`*timsol* **UNIX:** `/opt/IBM/TDI/V7.2/`*timsol*
Administrator account ID and password	An administrator account ID and password on the managed resource that has the rights to perform user provisioning on the IBM Security Secret Server and Thycotic Secret server adapter.	

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.

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.

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” on page 7.

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 `ThycoticConnector.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. 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.

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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

Creating an adapter service/target

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

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

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 `ThycoticConnector.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 `ThycoticConnector.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. 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.

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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

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

Verifying that the adapter is working correctly

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

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`
- `httpclient-4.5.2.jar`
- `httpcore-4.4.4.jar`
- `json-simple-1.1.1.jar`
- `commons-codec-1.9.jar`

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 `ThycoticConnector.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. 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.

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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

Creating an adapter service/target

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

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

Configuring the SSL connection between the IBM Security Directory Integrator and the IBM Security Secret Server and Thycotic Secret server

To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

About this task

For more infomration about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

Procedure

1. On a web browser, go to your instance URL. For example, `https://InstanceName/SecretServer`.
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 Secret Server and Thycotic Secret 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 thycotic -file c:\thycotic_cert.cer -keystore
     truststore.jks -storepass passw0rd
     ```
7. Edit `IDI_HOME/timsol/solution.properties` file to specify the truststore and keystore information.

   Note:

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

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

   If these key properties are not configured, you can set truststore to the same that contains the IBM Security Secret Server and Thycotic Secret server certificate. Otherwise, you must import the IBM Security Secret Server and Thycotic Secret server certificate to the truststore specified in `javax.net.ssl.trustStore` .
8. After you modify the `solution.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 `ThycoticConnector.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. 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.

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.

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 `ThycoticConnector.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 this installation is to upgrade a connector, then send a request from IBM Security Verify Identity. 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. 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.

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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

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

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

Restarting the adapter service

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

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

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

Related concepts

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

Verifying the adapter installation
If the adapter is installed correctly, the `ThycoticConnector.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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

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

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

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.

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 ThycoticConnector.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. 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.

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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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 16.

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

Service Target/Form details
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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

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

Verifying that the adapter is working correctly

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

Creating an adapter service/target

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

Before you begin

Complete the "Importing the adapter profile" on page 13

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 **Thycotic Adapter Service**.
4. Click **Next** to display the adapter service form.
5. Complete the fields on the service form. See "Service Target/Form details" on page 17.

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 `ThycoticConnector.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. 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.

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 Secret Server and Thycotic Secret server

To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must 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.

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 Details" on page 18
- "Connection Details tab" on page 18
- "Dispatcher Attributes tab" on page 18
- "Status and Information tab" on page 19

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 `ThycoticConnector.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. 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.

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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

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

Verifying that the adapter is working correctly

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

Service Details

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 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*.

Connection Details tab

This tab describes the parameters that have to be specified to establish a remote connection to the IBM Security Secret Server and Thycotic resource from IBM Security Directory Integrator.

Secret Server URL
Specify IBM Security Secret Server and Thycotic Secret serverURL of IBM Security Secret Server and Thycotic resource. For example, `https://<Instance-name>/SecretServer`

Secret Server User ID
Specify the administrator ID that can log in to the resource and perform user management operations. Ensure that the administrator user has sufficient privileges to perform user management operations.

Secret Server Password
Specify the password for administrator user.

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.

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 Secret Server and Thycotic resource is maintained. The next request that the adapter receives can reuse this connection.

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

Related concepts

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

Verifying the adapter installation
If the adapter is installed correctly, the `ThycoticConnector.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. 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.

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 Secret Server and Thycotic Secret server
To enable the communication between the adapter and the IBM Security Secret Server and Thycotic Secret server, you must configure the keystores for the Dispatcher.

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

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

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 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:

- `erTDIThycoticAccount.xml`
- `erTDIThycoticRMIService.xml`
- `TDIThycoticTest.xml`
- `TDIThycoticAdd.xml`
- `TDIThycoticSearch.xml`
- `TDIThycoticModify.xml`
- `TDIThycoticDelete.xml`
- `schema.dsml`
- `service.def`

Procedure

1. Edit the JAR file.
   a) Log on to the workstation where the IBM Security Secret Server and Thycotic Secret server 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 Secret Server and Thycotic Secret server adapter profile.

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

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

UNIX

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

b) Import the JAR file into the IBM Security Verify Identity 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.

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.

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 27 and Table 4 on page 27 contain warnings or errors, which might be displayed when the IBM Security Secret Server and Thycotic Secret server adapter is installed on your system.

Table 3. Specific messages and actions

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

Table 4. General messages and actions

Message	Action
`java.lang.NoClassDefFoundError: org.apache.http.client.ClientProtocolException`	The `httpclient-4.5.2.jar` file is missing. Verify that the file exists in the *ITDI_HOME*`/jars/3rdParty/IBM` directory.
`Adapter profile is not displayed in the user interface after installing the profile.`	You must stop and restart the Security Directory Integrator server or wait until the cache times out (up to 10 minutes) for IBM Security Verify Identity 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 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 Secret Server and Thycotic Secret server adapter supports a standard set of attributes for user information.

The mandatory attributes to create an account are:

- User Name
- User Display Name

Table 5. Supported Account attributes

IBM Security Secret Server and Thycotic Secret server adapter attribute name	Description	Required
eruid	userName	YES
erThycoticUserID	userID	NO
erThycoticDisplayName	displayName	YES
erThycoticLastLogin	lastLogin	NO
erThycoticCreatedDate	created	NO
erThycoticLoginFailures	loginFailures	NO
erThycoticEmailAddress	emailAddress	NO
erThycoticDomainID	domainId	NO
erThycoticIsLockedOut	isLockedOut	NO
erThycoticIsAppAccount	isApplicationAccount	NO
erThycoticUserGroup	assignedGroup	NO
erThycoticUserFolder	assignedFolder	NO
erThycoticSec	assignedSecret	NO

Supported Group Attributes

Table 6. Supported Group Attributes

IBM Security Secret Server and Thycotic Secret server adapter attribute name	Description	Required
erThycoticGroupID	groupid	YES
erThycoticGroupName	name	YES
erThycoticGroupDomainID	domainId	NO

Table 6. Supported Group Attributes (continued)		
IBM Security Secret Server and Thycotic Secret server adapter attribute name	**Description**	**Required**
erThycoticGroupDomainName	domainName	NO
erThycoticIsGroupEnabled	enabled	NO
erThycoticIsGroupSync	synchronized	NO
erThycoticGroupSec	assignedSecret	NO
erThycoticGroupFolder	assignedFolder	NO

Object Classes

Table 7. Supported object classes	
Description	**Object class name in schema**
Service class	**erTDIThycoticRMIService**
Account class	**erTDIThycoticAccount**
Group class	**erTDIThycoticGroup**
Secret class	**erTDIThycoticSecret**
Folder class	**erTDIThycoticFolder**

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 8. Add request	
Required attribute	**Optional attribute**
erUid	All other supported attributes
erThycoticDisplayName	

System Login Change

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

Table 9. Change request attribute	
Required attribute	**Optional attribute**
eruid	All other supported attributes

System Login Suspend

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

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

System Login Restore

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

Table 11. Restore request attributes	
Required attribute	**Optional attribute**
eruid	None
erAccountStatus	
erPassword	

System Change Password

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

Table 12. System change password request attributes	
Required attribute	**Optional attribute**
eruid	None
erPassword	

Test

The following table identifies attributes needed to test the connection.

Table 13. Test attributes	
Required attribute	**Optional attribute**
None	None

Reconciliation

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

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

Adapter Configuration Properties

For information about setting IBM Security Directory Integrator configuration properties for the operation of the IBM Security Secret Server and Thycotic Secret server adapter, see the *Dispatcher Installation and Configuration Guide*.

Index

A

account
  management automation 1
adapter
  account management automation 1
  attributes 31
  customization steps 23
  features 1
  installation
    connector 7, 8
    dispatcher requirement 7
    home directory 6
    overview 1
    solution directory 6
    troubleshooting errors 25
    verifying 20
    warnings 25
    worksheet 6
  overview 1
  profile
    removal 29
    upgrading 21
  supported configurations
    multiple server 1
    single server 1
  uninstallation 29
  upgrade 21
attributes
  mandatory 31
  standard 31
automation, account management 1

D

dispatcher
  installation 7
Dispatcher
  upgrades 21
download, software 5

E

error messages 26

I

installation
  adapter 7, 8
  dispatcher
    requirement 7
  first steps after
    adapter configuration 23
    adapter verification 23
    language pack installation 23
    SSL setup 23
installation *(continued)*
  planning roadmaps 3
  verification
    adapter 20
  worksheet
    home directory 6
    solution directory 6

M

messages
  error 26
  warning 26
MS-DOS ASCII characters 24

O

operating system prerequisites 4
overview 1

P

post-installation steps
  adapter configuration 23
  adapter verification 23
  language pack installation 23
  SSL setup 23
profile
  editing on UNIX or Linux 24
  removal 29

R

roadmaps
  planning 3

S

service
  restart 12
  start 12
  stop 12
software
  download 5
  requirements 4
  website 5
supported configurations
  adapter
    multiple server 1
    single server 1
  overview
    multiple server 1
    single server 1

T

troubleshooting
    error messages 26
    identifying problems 25
    techniques for 25
    warning messages 26
troubleshooting and support
    troubleshooting techniques 25

U

uninstallation
    adapter 29
    advance notice to users 29
updating
    adapter profile 23
upgrades
    adapter profiles 21
    Dispatcher 21

V

verification
    dispatcher installation 7
    installation 11, 20
    software
        prerequisites 4
        requirements 4
    system prerequisites 4
    system requirements 4
vi command 24

W

warning messages 26