IBM Security Verify Identity
7.0

Microsoft Office 365 Adapter Installation and Configuration Guide

IBM

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. Adapters might or might not be on the managed resource, and the Identity server manages access to the resource by using your security system.

The Microsoft Office 365 Adapter (Office 365 Adapter) uses the Security Directory Integrator functions to facilitate communication between the Identity server and Microsoft Office 365 (Office 365). The adapter functions as a trusted virtual administrator on the target platform. It does tasks such as creating login IDs, suspending IDs, and does other functions that administrators normally run manually.

Features of the adapter

This adapter automates several administrative tasks on the Office 365 domain.

You can use the adapter to automate the following tasks:

- Create, modify, suspend, restore, change password, and delete a user.
- Create, modify, and delete group.
- Reconcile user and user attributes.
- Reconcile group and group attributes.

Architecture of the adapter

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:

- The Dispatcher
- The IBM Security Directory Integrator connector
- IBM® Security Verify Adapter profile

You must install the Dispatcher and the adapter profile; however, the Security Directory Integrator connector might already be installed with the base Security Directory Integrator product.

The Office 365 Adapter consists of IBM Security Directory Integrator Assembly Lines. When an initial request is made by Identity server to the Office 365 Adapter, the assembly lines are loaded into the Security Directory Integrator server. Subsequent service requests do not require those same assembly lines to be reloaded.

The assembly lines use the Security Directory Integrator components to undertake user management-related tasks on the Office 365 domain. They do these tasks remotely by using the client id and key associated with a service principal object that has administrator privileges.

The following diagram shows the various components that work together to complete user management tasks in a Security Directory Integrator environment.
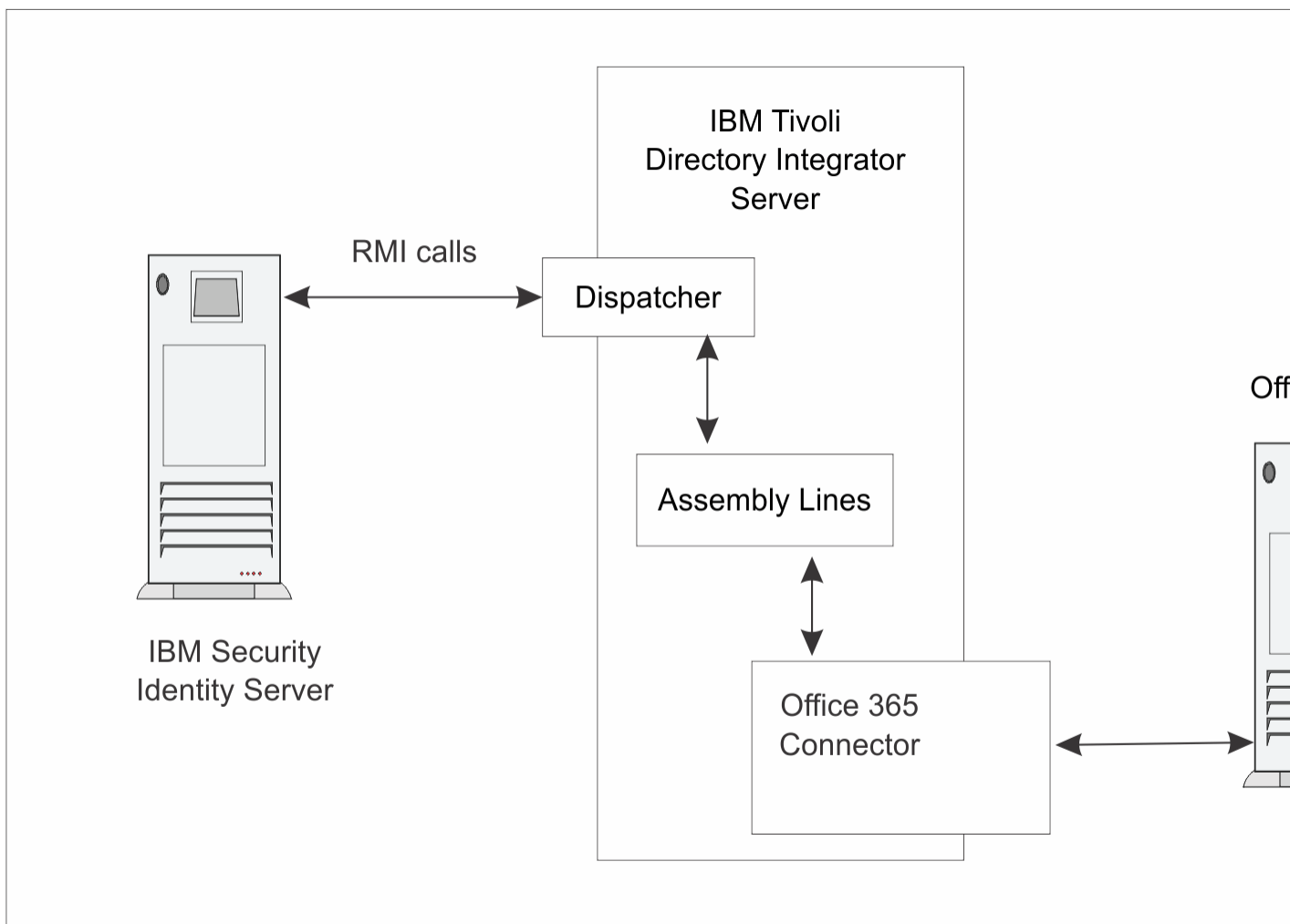
Figure 1. The architecture of the adapter

Supported configurations

The Office 365 Adapter supports a number of different configurations and is designed to operate with IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager.

The following components are the fundamental components of a Office 365 Adapter environment:

- An Identity server
- An IBM Security Directory Integrator server
- The Office 365 Adapter

As part of each configuration, the Office 365 Adapter must be installed on the computer that is running the IBM Security Directory Integrator server.

For a single server configuration, you must install the Identity server, IBM Security Directory Integrator server, and the Office 365 Adapter on one server. That server communicates with the Office 365 domain.

IBM Security
Identity Server

Tivoli Directory
Integrator Server

Adapter

Managed
resource
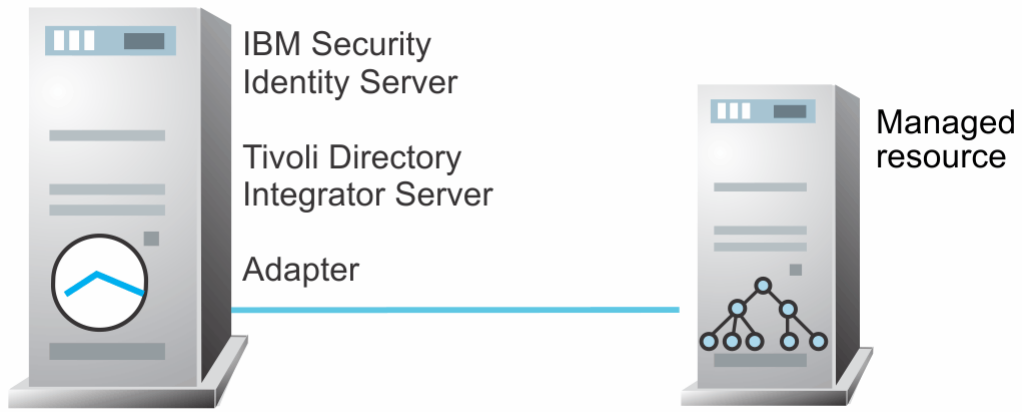
Figure 2. Single server configuration

Chapter 2. Planning

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

Use the Preinstallation roadmap to prepare the environment.

Table 1. Preinstallation road map	
Task	**For more information, see**
Verify that your environment meets the software and hardware requirements for the adapter.	"Prerequisites" on page 11.
Obtain the installation software.	Software download.
Obtain the necessary information for the installation and configuration.	"Installation worksheet" on page 13.

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

Table 2. Installation and configuration roadmap	
Task	**For more information, see**
Install the dispatcher.	Verifying the adapter installation.
Configure the Apache HttpComponent HttpClient Java Library	"Installing 3rd party client libraries" on page 15.
Install the connector.	"Installing the adapter binaries or connector" on page 15.
Configure the SSL connection between the Dispatcher and the Office 365 service.	"Configuring the SSL connection between the Dispatcher and the Office 365 domain" on page 16.
Import the adapter profile into the Identity server.	Importing the adapter profile.
Obtain an Application Id and Secret key for the adapter.	"Obtaining an Application Id and Secret key for the Office 365 Adapter" on page 26
Create an adapter service..	Creating an adapter service.

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

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

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Privileged Identity Manager

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

1. Install the dispatcher.
2. Install the adapter binaries or connector.
3. Install 3rd party client libraries.
4. Set up the adapter environment.
5. Restart the adapter service.
6. Import the adapter profile.
7. Create an adapter service/target.

8. Install the adapter language package.

9. Verify that the adapter is working correctly.

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.

   a. Configure 1-way authentication.

   b. Configure 2-way authentication.

2. Configure secure communication between the adapter and the managed target.

   a. Configure 1-way authentication.

   b. Configure 2-way authentication.

3. Configure the adapter.

4. Modify the adapter profiles.

5. Customize the adapter.

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

1. Stop the adapter service.

2. Remove the adapter binaries or connector.

3. Remove 3rd party client libraries.

4. Delete the adapter service/target.

5. Delete the adapter profile.

Reference

See the following topics.

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

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Prerequisites

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

Ensure that you install the adapter on the same workstation as the Security Directory Integrator server.

Table 3. Prerequisites to install the adapter	
Prerequisite	**Description**
Operating system	The Office 365 Adapter can be used on any operating system that is supported by Security Directory Integrator.
Network Connectivity	Internet Protocol network
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.

Table 3. Prerequisites to install the adapter (continued)

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: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0
Dispatcher	Obtain the dispatcher installer from the IBM Passport Advantage website.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. For more information, see the *Dispatcher Installation and Configuration Guide*.
Apache HttpComponent HttpClient Java library	See the *Office 365 Adapter Release Notes* for the supported API package name and version.
SSL Configuration	Ensure that the MSIT Machine Auth CA2, `login.windows.net` and `graph.windows.net` certificates are in place.

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1.1: Installation and Administrator Guide*.

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 IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

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

Table 4. Required information to install the adapter		
Required information	**Description**	**Value**
Client ID and key	A client ID and key that is associated with a service principal object on the managed resource that has administrative rights for running the Office 365 Adapter.	

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the jars/connectors subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Security Directory Integrator is automatically installed with your IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager product, the default directory path for Security Directory Integrator is as follows:
		
		Windows:
		
		• for version 7.1.1:
		
		  drive`\Program Files\IBM`
		  `\TDI\V7.1.1`
		
		UNIX:
		
		• for version 7.1.1:
		
		  `/opt/IBM/TDI/V7.1.1`

Adapters solution directory	When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at:
		
		Windows:
		
		• for version 7.1.1:
		
		  drive`\Program Files\IBM`
		  `\TDI\V7.1.1\`*timsol*
		
		UNIX:
		
		• for version 7.1.1:
		
		  `/opt/IBM/TDI/V7.1.1/`
		  timsol

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.

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.*

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 extract the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `O365Connector.jar` file to the *ITDI_HOME*`/jars/connectors` directory.
4. Restart the adapter service.

Installing 3rd party client libraries

The adapter requires access to the Apache HttpComponent HttpClient Java Library at run time.

Before you begin
The Java library must be downloaded from the http://hc.apache.org/index.html website.

Procedure

1. Go to the http://hc.apache.org/index.html website. Under **Download**, search for the **HttpComponents Client** package that is listed in the *Office 365 Adapter Release Notes*.
2. Download the **HttpComponents Client** package to a temporary directory.
3. Copy these files to *ITDI_HOME*`\jars\patches` directory.

   Note: In the previous versions of the adapter, the files must be copied to *ITDI_HOME*`\jvm\jre\lib\ext`. Use the new location *ITDI_HOME*`\jars\patches` instead.

   See the *Office 365 Adapter Release Notes* for the path to these JAR files in the package.

- `commons-logging-1.1.1.jar`
- `httpclient-4.2.X.jar`
- `httpcore-4.2.X.jar`

4. Restart the Dispatcher service.

   For information about starting and stopping the service, see the *Dispatcher Installation and Configuration Guide.*

Setting up the adapter environment

In addition to 3rd party client libraries, some adapter require file system and operating system configuration.This topic is not applicable for this adapter.

About this task

Procedure

Configuring the SSL connection between the Dispatcher and the Office 365 domain

To enable communication between the adapter and the Office 365 domain, you must configure keystores for the Dispatcher.

About this task

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

Procedure

1. Open a browser.
2. Go to https://accounts.accesscontrol.windows.net

   Note: The Internet Explorer browser might return a HTTP 400 Bad Request message. You might be unable to view the SSL lock button. To correct this issue:

   a. On the browser, go to **Tools > Internet Options** and click the **Advanced** tab.

   b. In the **Settings** panel, locate the **Show friendly HTTP error messages** option under **Browsing**.

   c. Disable the **Show friendly HTTP error messages** option.

   d. Click **Apply** and then click **OK** to close the panel.

   e. Click the **Refresh** button to reload the link and display the SSL lock.

3. View the certificate.

   - Click **SSL lock**.
   - If your browser reports that revocation information is not available, click **View Certificate**.

4. Click **Certification Path**
5. Select the **MSIT Machine Auth CA 2** certificate.
6. Export the certificate into a file that is encoded in the Base64 format.
7. If the Dispatcher already has a configured keystore, use the iKeyman Utility to import the **MSIT Machine Auth CA 2** certificate. Complete the following steps:

   a) Navigate to the *ITDI_HOME*/jvm/jre/bin directory.

   b) Start the **ikeyman.exe** file.

   c) From the **Key Database File** menu, select **Open**.

d) For the key database type, select **JKS**.

e) Type the keystore file name: **testadmin.jks**.

f) Type the location: *ITDI_HOME*/timsol/serverapi.

g) Enter the password when prompted. The default password is **administrator**.

h) Click **Signer Certificates** in the dropdown menu and click **Add**.

i) Use **Browse** to select the downloaded or exported **MSIT Machine Auth CA 2** certificate.

j) Click **OK** to continue. The certificate is added in the certificate store.

k) Restart the Dispatcher service and browser.

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

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*.

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

Procedure

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

4. On the **Import Service Type** page, complete these steps:

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

   b) Click **OK** to import the file.

Results

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

What to do next

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

Importing the adapter profile

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

Before you begin

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

About this task

Service definition files are also called adapter profile files.

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

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

Procedure

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

The **Import Service Type** page is displayed.

4. On the **Import Service Type** page, complete these steps:

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

   b) Click **OK** to import the file.

Results

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

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.

- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the **handler.file.fileDir** property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server*HOME*`\data` directory. .

Importing the adapter profile

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

Before you begin

- The IBM Security Privileged Identity Manager is installed and running.

- You have root or administrator authority on the IBM Security Privileged Identity Manager.

- 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 Privileged 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 IBM Security Privileged Identity Manager 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. .

Importing the adapter profile

You can import a profile definition file, which creates a profile in Identity server. Use this option for importing adapter profiles.

Before you begin

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

About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Verify Adapter. The adapter profile must be imported because it defines the types of resources that the Verify Governance Identity Manager server can manage.

The adapter profile definition file is used to create a target profile on the Verify Governance Identity Manager server and to establish communication with the adapter. If the adapter profile is not imported, you cannot create a connector for that adapter type.

An upload error might occur when no file is selected, or when the file is empty, or due to any upload operation error, such as a timeout or connection error. If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a connector with the adapter profile or open and account on the service. You must import the adapter profile again.

This task can be completed from the Enterprise Connectors module in the Administration Console. To import an adapter target profile, complete these steps:

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.

2. From the Administration Console, select **Enterprise Connectors**.

3. Select **Manage** > **Profiles**.

4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

5. Click **Actions** > **Import**.

6. On the **Import** page, complete these steps:

   a) Select **Profile**.

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

   c) Click **Upload file**.

   A message indicates that you successfully imported a profile.

7. Click **Close**.

   The new profile is displayed in the list of profiles.

Results

The upload is synchronous but has a timeout. The progress bar on the **Import** page accurately indicates the upload status. However, when a timeout is reached, the following message occurs: "The import is still in progress and will complete shortly. Close this window to proceed." If you see that message, allow a few minutes for the upload to complete and for the profile to be available.

What to do next

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

- Import the attribute mapping file. See "Importing attribute mapping file" on page 21.
- Create a connector that uses the target profile. See "Adding a connector" on page 23.

Importing attribute mapping file

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

About this task

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

Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.

2. From the Administration Console, select **Enterprise Connectors**.

3. Select **Manage** > **Profiles**.

4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

5. Click **Actions** > **Import**.

6. On the **Import** page, complete these steps:

   a) Select **Attribute Mapping**.

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

   c) Click **Upload file**.

   A message indicates that you successfully imported the file.

7. Click **Close**.

Enabling connectors

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

Before you begin

Table 5. Prerequisites for enabling a connector	
Prerequisite	**Find more information**
A connector must exist in Verify Governance Identity Manager.	"Adding a connector" on page 23.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 24.

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:

   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

      Enable write-to channel
      Propagates every change in the Access Governance Core repository into the target system.

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

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

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

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

Results

The connector is enabled

What to do next

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

Adding a connector

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

Before you begin

Complete Importing the adapter profile.

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

About this task

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

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

Procedure

To add a connector, complete these steps.
1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions** > **Add**.

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

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

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

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

      For information about the global configuration properties, see Global Config accordion pane.
   h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

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

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

What to do next

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

Reviewing and setting channel modes for each new connector

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

About this task

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

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

Procedure

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

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage** > **Connectors**.

   A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:

   a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.

   Enable write-to channel
   Propagates every change in the Access Governance Core repository into the target system.

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

   Enable reconciliation
   Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor** > **Change Log Sync Status**.

   A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:

   a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

   b) Select a connector, and click **Actions** > **Sync Now**.

   The synchronization process begins.

   c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.

   Information about the synchronization is displayed in the **Sync History** tab.

10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
    a) Select **Manage** > **Connectors**.
    b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    c) Click **Save**.

       For more information, see "Enabling connectors" on page 22.

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

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

Attribute Mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.

6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

Obtaining an Application Id and Secret key for the Office 365 Adapter

Before you create an Office 365 service, you must obtain an Application Id and Secret key for the Office 365 Adapter.

About this task
The Office 365 Adapter authenticates to the Office 365 domain through the Windows Azure Active Directory Graph API using OAuth 2.0 Client credentials.

Procedure

1. Register the Office 365 Adapter as an application using the Azure Active Directory management Portal.

   For details of the application registration process, see the https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app.

2. Office 365 Adapter requires the following permissions for applications on the Azure Active Directory management Portal:

   Delegated permission- Office 365 graph

   - Directory.AccessAsUser.All
   - Directory.Read.All
   - Directory.ReadWrite.All
   - Group.Read.All
   - Group.ReadWrite.All
   - User.Read
   - User.Read.All
   - User.ReadBasic.All

   Delegated permission- Application permission

   - Directory.Read.All
   - Directory.ReadWrite.All

   Microsoft Graph

   - Directory.ReadWrite.All
   - User.ReadWrite.All

   To DELETE USER and CHANGE PASSWORD on the Microsoft Office 365, a "User Administrator Role" must be assigned to the AD application.
   To assign this role, follow steps below:

   a. Sign in to the Azure portal.

b. Switch to the directory, **Roles and Administrators**.

c. Select the **User administrator role**.

d. Click **Add assignment**.

e. In the **Select** text box, specify the name of the application that is registered earlier. For example, Test_APP. From the search results, select the required application.

f. Click **Add**. Permissions might take a few minutes to be fully propagated.

To delete role membership of user, assign "Global Administrative role" to AD application on Azure
To assign this role, follow steps below:

a. Sign in to the Azure portal.

b. Switch to the directory, **Roles and Administrators**.

c. Select the **Global administrator role**.

d. Click **Add assignment**.

e. In the **Select** text box, specify the name of the application that is registered earlier. For example, Test_APP. From the search results, select the required application.

f. Click **Add**. Permissions might take a few minutes to be fully propagated.

3. After the adapter is registered, obtain the Application ID and Secret key and use them as the client ID and password for authentication.

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 "Importing the adapter profile" on page 17.

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. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.

If the table contains multiple pages, you can do the following tasks:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

    c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.

The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.

5. On the **Select the Type of Service** page, select a service type, and then click **Next**.

If the table contains multiple pages, you can do the following tasks:

- Click the arrow to go to the next page.
- Type the number of the page that you want to view and click **Go**.

6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.

The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.

7. To create a service with NTLM authentication, the administrator login is in the following format:

```
<Domain Name>\<Login Name>
```

8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.

9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.

10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

Specify the expected access information and any other optional information such as description, search terms, more information, or badges.

11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

The adapter must be running to obtain the information.

12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.

13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.

14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

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 "Importing the adapter profile" on page 18.

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. From the navigation tree, click **Manage Services**.

   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.

   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.

   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.

      A list of business units that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:
      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.
   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.

      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.

   If the table contains multiple pages, you can do the following tasks:
   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.

The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.

7. To create a service with NTLM authentication, the administrator login is in the following format:

```
<Domain Name>\<Login Name>
```

8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.

9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.

    The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.

10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

    Specify the expected access information and any other optional information such as description, search terms, more information, or badges.

11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

    The adapter must be running to obtain the information.

12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

    The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.

13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

    The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.

14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

    If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

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 "Importing the adapter profile" on page 19.

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. From the navigation tree, click **Manage Services**.

   The **Select a Service** page is displayed.

2. On the **Services** table, click **Create**.

   The **Create a Service** wizard is displayed.

3. On the **Select the Type of Service** page, click **Search** to locate a business unit.

   The **Business Unit** page is displayed.

4. On the **Business Unit** page, complete these steps:

   a) Type information about the business unit in the **Search information** field.

   b) Select a business type from the **Search by** list, and then click **Search**.

      A list of business units that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.

      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.

5. On the **Select the Type of Service** page, select a service type, and then click **Next**.

6. On the **Service Information** page, specify the appropriate values for the service instance.

   The content of the **Service Information** page depends on the type of service that you are creating.

7. Click **Test Connection** to validate that the data in the fields is correct.

   If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

8. Click **Finish**.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

Service/Target form details

Complete the service/target form fields.

You must create an administrative user account for the adapter on the managed resource. Specify an immutable ID in case of creating an account in federated domain. The default password policy for user provisioning has been strengthened. See the Microsoft Office 365 online portal for more information.

Adapter Details

   Service Name

   Specify a name that defines the adapter service on the Identity server.

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

   Description

   Specify a description that identifies the service for your environment.

Security Directory Integrator location

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

The default URL for the default SDI1 instance is `rmi://localhost:1099/ITDIDispatcher`.

The following table shows the ports that are open in the firewall for every instance that is created. However, usage of these port numbers do not support high availability.

Table 6. Ports	
Instance	**Ports**
SDI1	1199, 1198, 1197, 1196, 1195, 1194
SDI2	2299, 2298, 2297, 2296, 2295, 2294
SDI3	3399, 3398, 3397, 3396, 3395, 3394
SDI4	4499, 4498, 4497, 4496, 4495, 4494
SDI5	5599, 5598, 5597, 5596, 5595, 5594
SDI6	6699, 6698, 6697, 6696, 6695, 6694
SDI7	7799, 7798, 7797, 7796, 7795, 7794
SDI8	8899, 8898, 8897, 8896, 8895, 8894
SDI9	9999, 9998, 9997, 9996, 9995, 9994
SDI10	11099, 11098, 11097, 11096, 11095, 11094

For a high availability implementation, use any of these port numbers.

- 1099
- 2099
- 3099

Owner

Specify a user as a service owner. Click **Search** to find the user ID that you want to specify as the owner of the service.

Service prerequisite

Specify a service that is prerequisite to this service. Click **Search** to specify an existing service instance or function that the Office 365 service instance requires.

Office 365 Domain Details

Office 365 domain name

Specify the name of the Office 365 domain.

Application Id

Specify the application id contained in the application credential that is associated with the service principal object that represents the Office 365 adapter service.

Application key

Specify the application secret that is contained in the application credential that is associated with the service principal object that represents the Office 365 adapter service.

Proxy Server host

Specify the host name or IP address of the proxy server.

Proxy Server port

Specify the port number for the proxy server.

Search Page Size (1-999)
Specify a search page size for reconciliation.

Dispatcher Attributes

AL FileSystem 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 Identity server. You can specify a file path to load the assembly lines from the `profiles` directory of the Windows operating system such as: `drive:\Program Files\IBM\TDI\V7.1.1\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating system: `/opt/IBM/TDI/V7.1.1/profiles`

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. Enter 10 when you want the dispatcher to run a maximum of 10 assembly lines simultaneously for the service. If you enter 0 in the **Max Connection Count** field, the dispatcher does not limit the number of assembly lines that are run simultaneously for the service.

Disable AL Caching
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add, modify, delete, and test operations are not cached.

Status and information
The page 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 that the adapter is connected to.

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 Identity server.

TDI version
Specifies the version of the 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 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.

If the connection fails, follow the instructions in the error message. Also

• Verify the adapter log to ensure that the test request was sent successfully to the adapter.

- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. Verify parameters such as the work station name or the IP address of the managed resource and the port.

Installing the adapter language package

The adapters use a separate language package from IBM Security Verify Identity.

See *Installing the adapter language pack* from the IBM Security Verify Identity product documentation.

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.

   The default password policy for user provisioning has been strengthened. Please refer to the Office 365 online portal for further details.

Chapter 4. Configuring

After you install the adapter, configure it to function correctly.

- Use the new User Domain Name attribute to view which domain to create the user when you are specifying the User Principal Name.

- The User Id attribute is now replaced by the User Principal Name attribute. This attribute requires an input string in the format of `username@userDomainName.com`. To assign a user to a domain, replace the `UserDomainName` of the User Principal Name with a different domain name. The `UserDomainName` of the User Principal Name must match the value that is specified in the User Domain Name attribute.

Chapter 5. Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Related concepts

Error messages and problem solving
You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Error messages and problem solving

You might encounter some problems at run time. Use this information to resolve some of these common runtime problems.

Runtime problems and corrective actions are described in the following table.

Table 7. Runtime problems	
Problem	**Corrective Action**
Reconciliation does not return all Office 365accounts. Reconciliation is successful but some accounts are missing.	For the adapter to reconcile many accounts successfully, you must increase the WebSphere JVM memory. Do the following steps on the WebSphere host computer: **Note:** Do not increase the JVM memory to a value higher than the system memory. 1. Log in to the administrative console. 2. Expand **Servers** in the left menu and select **Application Servers**. 3. A table contains the names of known application servers on your system. Click the link for your primary application server. 4. Select **Process Definition** from the **Configuration** tab. 5. Select the `Java Virtual Machine` property. 6. Enter a new value for the `Maximum Heap Size`. The default value is 256 MB. If the allocated JVM memory is not large enough, an attempt to reconcile many accounts with the adapter results in log file errors. The reconciliation process fails. The adapter log files contain entries that state `ErmPduAddEntry failed`. The `WebSphere_install_dir`/logs/itim.log file contains **java.lang.OutOfMemoryError** exceptions.

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 6. Uninstalling

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

Removing the adapter binaries or connector

Use this task to remove the connector file for the Office 365 Adapter.

About this task

To uninstall the Dispatcher, see the *Dispatcher Installation and Configuration Guide*.

To remove the Office 365 Adapter, complete these steps:

Procedure

1. Stop the Dispatcher service.
2. Delete the *ITDI_HOME*/jars/connectors/O365Connector.jar file.
3. Delete the following JAR files from the *ITDI_HOME*\jars\patches directory.

   ```
   commons-logging-1.1.1.jar
   httpclient-4.2.X.jar
   httpcore-4.2.X.jar
   ```

4. Start the Dispatcher service.

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 IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager product documentation.

Chapter 7. Reference

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

Adapter attributes and object classes

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network. After you install the adapter profile, the Office 365 Adapter supports a standard set of attributes.

User attributes

The following tables show the standard attributes and object classes that are supported by the Office 365 Adapter.

Table 8. Supported user attributes

IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager name	Attribute name in schema	Data type
User Principal Name	eruid	String
Password	erpassword	Password
Display Name	ero365displayname	String
Mail Nickname	ero365mailnickname	String
Change Password on Next Login	ero365chgpwdnextlogin	String
Given Name	ero365givename	String
Last Name	ero365surname	String
Mail	ero365mail	String
Job Title	ero365jobtitle	String
Department	ero365department	String
Office Number	ero365office	String
Office Phone	ero365telphone	String
Mobile Phone	ero365mobile	String
Fax Number	ero365fax	String
Street Address	ero365street	String
City	ero365city	String
State or Province	ero365state	String
Zip or Postal Code	ero365postalcode	String
Country or Region	ero365country	String
Preferred Language	ero365preflang	String

Table 8. Supported user attributes (continued)		
IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager name	**Attribute name in schema**	**Data type**
Set User Location	ero365location	String
Assign Licenses	ero365licvalue	String
Alternate Email Address	ero365othermail	String
Group Membership	ero365groupoid	String
Administrator Role Membership	ero365roleoid	String
User Domain Name	ero365userdomainname	String

Group attributes

Table 9. Supported group attributes		
IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager name	**Attribute name in schema**	**Data type**
Group Id	ero365groupoid	String
Group Name	ero365groupdisplayname	String
Group Description	ero365groupdesc	String

Note:

- The **Group Id** attribute is the Object Id of the Office 365 group. This attribute is mapped to the IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager **erGroupId**. You cannot use the adapter to modify this attribute.
- The **Group Name** attribute is mapped to the IBM Security Verify IdentityIBM Security Verify Governance Identity ManagerIBM Security Privileged Identity Manager **erGroupName** attribute. You cannot user the adapter to modify this attribute.

Object classes

Table 10. Supported object classes		
Description	**Object class name in schema**	**Superior**
Service class	ero365service	Top
Account class	ero365account	Top
Group class	ero365groups	Top
License class	ero365licenses	Top

Adapter configuration properties

For information about setting Security Directory Integrator configuration properties for the operation of the Office 365 Adapter, see the *Dispatcher Installation and Configuration Guide*.

Index

A

adapter
    features 1
    installation
        worksheet 13
    overview 1
    uninstall 41
adapters
    removing profiles 41
Apache HttpComponent HttpClient Java Library 15
architecture 1
automation of administrative tasks 1

C

components 2
configuration
    for SSL 16
connector files, removing 41

D

dispatcher
    architecture 1
    installation 15
download, software 12

I

installation
    adapter 15
    language pack 34
    uninstall 41
    worksheet 13

L

language pack
    installation 34
    same for adapters and server 34

O

overview, adapter 1

R

removing
    adapter profiles 41
    connector files 41

S

service

service (continued)
    restart 17
    start 17
    stop 17
software
    download 12
    website 12
supported configurations 2

T

task automation 1
tivoli directory integrator connector 1
troubleshooting
    identifying problems 37
    runtime problems 38
    techniques for 37
troubleshooting and support
    troubleshooting techniques 37

U

uninstallation, directory integrator 41

V

verification
    dispatcher installation 15