

IBM Security Verify Governance Identity
Manager
10.0

*Microsoft Azure Active Directory Adapter
Installation and Configuration Guide*



Contents

Figures.....	v
Tables.....	vii
Chapter 1. Overview.....	1
Features of the adapter.....	1
Architecture of the adapter.....	1
Supported configurations.....	2
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.....	7
Installing 3rd party client libraries.....	7
Restarting the adapter service.....	8
Configuring the SSL connection between the Dispatcher and the Azure Active Directory domain.....	8
Importing the adapter profile.....	8
Obtaining an Application ID and Secret key for the Azure Active Directory Adapter.....	9
Creating an adapter service/target.....	11
Service/Target form details.....	12
Installing the adapter language package.....	14
Verifying that the adapter is working correctly.....	14
Chapter 4. Troubleshooting.....	15
Techniques for troubleshooting problems.....	15
Error messages and problem solving.....	16
Chapter 5. Uninstalling.....	19
Removing the adapter binaries or connector.....	19
Deleting the adapter profile.....	19
Chapter 6. Reference.....	21
Adapter attributes and object classes.....	21
Adapter attributes by operations.....	22
Special attributes.....	23
Index.....	25

Figures

- 1. The architecture of the Azure Active Directory adapter..... 2
- 2. Single server configuration.....2

Tables

1. Prerequisites to install the adapter.....	4
2. Required information to install the adapter.....	6
3. Runtime problems.....	17
4. Supported user attributes.....	21
5. Supported group attributes.....	22
6. Supported object classes.....	22

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The Microsoft Azure Active Directory (Azure Active Directory Adapter) uses the Security Directory Integrator functions to facilitate communication between the Identity server and Microsoft Azure Active Directory (Azure Active Directory).

Adapters can be installed on the managed resource. The Identity server manages access to the resource by using the security system. Adapters function as trusted virtual administrators on the target operating system. The adapter creates, suspends, restores user accounts, and other functions that administrators run manually. The adapter runs as a service, independently of whether you are logged on to the Identity server.

Features of the adapter

The adapter automates several administrative and management tasks.

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 RMI 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 Azure Active Directory Adapter consists of IBM Security Directory Integrator Assembly Lines. When an initial request is made by Identity server to the Azure Active Directory 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 Azure Active Directory domain. They do these tasks remotely by using the client id and client secret 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.

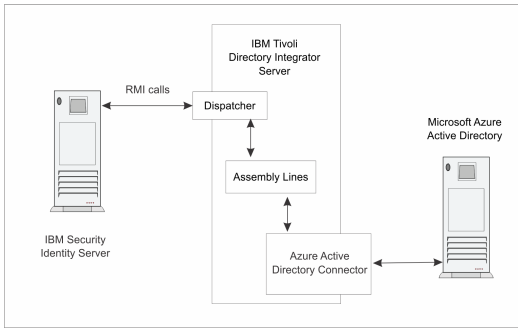


Figure 1. The architecture of the Azure Active Directory adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The following components are the fundamental components of a Azure Active Directory Adapter environment:

- An Identity server
- An IBM Security Directory Integrator server
- The Azure Active Directory Adapter

As part of each configuration, the Azure Active Directory 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 Azure Active Directory Adapter on one server. That server communicates with the Azure Active Directory domain.

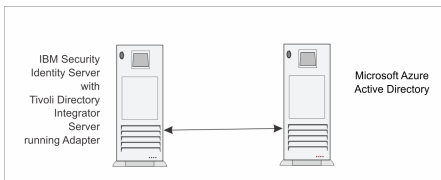


Figure 2. Single server configuration

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.

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

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.

Use the Preinstallation roadmap to prepare the environment.

Prerequisite	Description
Operating system	The Azure Active Directory 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 1. Prerequisites to install the adapter (continued)

Prerequisite	Description
Directory Integrator	<ul style="list-style-type: none"> IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 IBM® Security Directory Integrator Version 7.2 <p>Note:</p> <ul style="list-style-type: none"> 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	<p>The following servers are supported:</p> <ul style="list-style-type: none"> 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	<p>A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for IBM Security Verify Adapters.</p> <p>For more information, see the <i>Dispatcher Installation and Configuration Guide</i>.</p>
Apache HttpComponent HttpClient Java library	See the <i>Azure Active Directory Adapter Release Notes</i> for the supported API package name and version.
SSL Configuration	DigiCert Global Root CA Certificate. See Configuring the SSL connection between the Dispatcher and the Azure Active Directory domain .

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 Governance 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.

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 Azure Active Directory Adapter.	
Security Directory Integrator Home Directory	The <i>ITDI_HOME</i> directory contains the <i>jars/connectors</i> subdirectory that contains adapter JAR files. For example, the <i>jars/connectors</i> subdirectory contains the JAR file for the UNIX adapter.	<p>If Security Directory Integrator is automatically installed with your Identity server product, the default directory path for Security Directory Integrator is as follows:</p> <p>Windows:</p> <ul style="list-style-type: none"> for version 7.1.1: <i>drive\Program Files\IBM\TDI\V7.1.1</i> <p>UNIX:</p> <ul style="list-style-type: none"> for version 7.1.1: <i>/opt/IBM/TDI/V7.1.1</i>
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 <i>Dispatcher Installation and Configuration Guide</i> .	<p>The default solution directory is at:</p> <p>Windows:</p> <ul style="list-style-type: none"> for version 7.1.1: <i>drive\Program Files\IBM\TDI\V7.1.1\timsol</i> <p>UNIX:</p> <ul style="list-style-type: none"> for version 7.1.1: <i>/opt/IBM/TDI/V7.1.1/timsol</i>

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 [Verifying the adapter installation](#).

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 `AzureADConnector.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 *Azure Active Directory 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 *Azure Active Directory 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*.

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*.

Configuring the SSL connection between the Dispatcher and the Azure Active Directory domain

To enable communication between the adapter and the Azure Active Directory 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. Navigate to <https://www.digicert.com/kb/digicert-root-certificates.htm>.
3. Select **DigiCert Global Root CA Certificate**.
4. Download the certificate.
5. If the Dispatcher already has a configured keystore, use the iKeyman Utility to import the **DigiCert Global Root CA Certificate**. Complete the following steps:
 - a) Use Browse to select the downloaded or exported **DigiCert Global Root CA** certificate.

For information about SSL configuration, see 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

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

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. .

Obtaining an Application ID and Secret key for the Azure Active Directory Adapter

Before you create an Azure Active Directory service, you must obtain an Application Id and Secret key for the Azure Active Directory Adapter.

About this task

The Azure Active Directory Adapter authenticates to the Azure Active Directory domain through the Windows Azure Active Directory Graph API using OAuth 2.0 Client credentials.

To delete user and change password on the Azure Active Directory Adapter, a "User Administrator Role" must be assigned to the AD application

Take the following steps, to assign this role:

1. Sign in to the Azure Active Directory portal.
2. Switch to **Roles and Administrators**.
3. Select the **User administrator role**.

4. Click **Add assignment**.
5. 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.
6. 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 Active Directory

Take the following steps, to assign this role:

1. Sign in to the Azure Active Directory portal.
2. Switch to **Roles and Administrators**.
3. Select the **Global administrator role**.
4. Click **Add assignment**.
5. 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.
6. Click **Add**. Permissions might take a few minutes to be fully propagated.

Procedure

1. Register the Azure Active Directory Adapter as an application by logging into the Azure management Portal as an administrator.
For more details on the application registration process, see <https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app>.
2. Azure Active Directory Adapter requires the following permissions for applications on the Azure management Portal:

Delegated permission- Azure Active Directory 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

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 8.

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.

Service/Target form details

Complete the service/target form fields.

Azure Active Directory Domain Details

Azure Active Directory domain name

Specify the name of the Azure Active Directory domain.

Application Id

Specify the application id contained in the application credential that is associated with the service principal object that represents the Azure Active Directory 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 Azure Active Directory 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.

Enable TDI detailed debugging

Click the check box to enable the detailed log option of the assembly line. Clear the check box to disable the option.

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 Governance Identity Manager.

See *Installing the adapter language pack* from the [IBM Security Identity Manager](#) 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.

Chapter 4. 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 3. Runtime problems

Problem	Corrective Action
<p>Reconciliation does not return all Azure Active Directory accounts. Reconciliation is successful but some accounts are missing.</p>	<p>For the adapter to reconcile many accounts successfully, you must increase the WebSphere JVM memory. Do the following steps on the WebSphere host computer:</p> <p>Note: Do not increase the JVM memory to a value higher than the system memory.</p> <ol style="list-style-type: none"> 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. <p>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.</p> <p>The adapter log files contain entries that state <code>ErmpduAddEntry failed</code>. The <code>WebSphere_install_dir/logs/itim.log</code> file contains java.lang.OutOfMemoryError exceptions.</p>

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 5. 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 Azure Active Directory Adapter.

About this task

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

To remove the Azure Active Directory Adapter, complete these steps:

Procedure

1. Stop the Dispatcher service.
2. Delete the `ITDI_HOME/jars/connectors/AzureADConnector.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 Governance Identity Manager product documentation.

Chapter 6. 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 Azure Active Directory Adapter supports a standard set of attributes.

User attributes

The following tables show the standard attributes and object classes that are supported by the Azure Active Directory Adapter.

Table 4. Supported user attributes

IBM Security Verify Governance Identity Manager name	Attribute name in schema	Data type
User ID	eruid	String
Password	erpassword	Password
Display Name	erazuredisplayname	String
Mail Nickname	erazuremailnickname	String
Change Password on Next Login	erazurechgpwdnextlogin	String
Given Name	erazuregivenname	String
Last Name	erazuresurname	String
Mail	erazuremail	String
Job Title	erazurejobtitle	String
Department	erazuredepartment	String
Office Number	erazureoffice	String
Office Phone	erazuretelephone	String
Mobile Phone	erazuremobile	String
Fax Number	erazurefax	String
Street Address	erazurestreet	String
City	erazurecity	String
State or Province	erazurestate	String
Zip or Postal Code	erazurepostalcode	String
Country or Region	erazurecountry	String
Preferred Language	erazurepreflang	String
Set User Location	erazurelocation	String
Assign Licenses	erazurelicvalue	String

Table 4. Supported user attributes (continued)

IBM Security Verify Governance Identity Manager name	Attribute name in schema	Data type
Alternate Email Address	erazureothermail	String
Group Membership	erazuregroupoid	String
Administrator Role Membership	erazureroleoid	String

Group attributes

Table 5. Supported group attributes

IBM Security Verify Governance Identity Manager name	Attribute name in schema	Data type
Group Id	erazuregroupoid	String
Group Name	erazuregroupdisplayname	String
Group Description	erazuregroupdesc	String

Note:

- The **Group Id** attribute is the Object Id of the Azure Active Directory group. This attribute is mapped to the IBM Security Verify Governance Identity Manager **erGroupId**. You cannot use the adapter to modify this attribute.
- The **Group Name** attribute is mapped to the IBM Security Verify Governance Identity Manager **erGroupName** attribute. You cannot use the adapter to modify this attribute.

Object classes

Table 6. Supported object classes

Description	Object class name in schema	Superior
Service class	erazureservice	Top
Account class	erazureaccount	Top
Group class	erazuregroups	Top
License class	erazurelicenses	Top

Adapter configuration properties

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

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. This topic is not applicable for this adapter.

Special attributes

Certain attributes have special syntax and meaning that customers needs to be aware off. This information will be used to help the customer in how to supply the attribute value.This topic is not applicable for this adapter.

Index

A

adapter
 features [1](#)
 installation
 planning [3](#)
 troubleshooting errors [15](#)
 verifying [14](#)
 warnings [15](#)
 worksheet [6](#)
 overview [1](#)
 uninstall [19](#)
adapters
 removing profiles [19](#)
Apache HttpComponent HttpClient Java Library [7](#)
architecture [1](#)
attributes
 group [21](#)
 user [21](#)
automation of administrative tasks [1](#)

C

components [2](#)
configuration
 properties [21](#)

D

dispatcher
 architecture [1](#)
 installation [7](#)
download, software [5](#)

G

group attributes [21](#)

I

installation
 adapter [7](#)
 language pack [14](#)
 uninstall [19](#)
 verification
 adapter [14](#)
 worksheet [6](#)

L

language pack
 installation [14](#)
 same for adapters and server [14](#)

O

object classes [21](#)
overview, adapter [1](#)

P

planning installation [3](#)

R

removing
 adapter profiles [19](#)

S

service
 restart [8](#)
 start [8](#)
 stop [8](#)
software
 download [5](#)
 website [5](#)
supported configurations [2](#)

T

task automation [1](#)
tivoli directory integrator connector [1](#)
troubleshooting
 identifying problems [15](#)
 runtime problems [16](#)
 techniques for [15](#)
troubleshooting and support
 troubleshooting techniques [15](#)

U

user attributes [21](#)

V

verification
 dispatcher installation [7](#)
 installation [14](#)

