IBM Security Identity Governance and Intelligence

Microsoft Office 365 Adapter Installation and Configuration Guide

IBM Security Identity Governance and Intelligence

Microsoft Office 365 Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

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

The Microsoft Office 365 Adapter (Office 365 Adapter) uses the Tivoli® Directory Integrator functions to facilitate communication between the IBM Security 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 Tivoli Directory Integrator connector
- IBM Security Identity Adapter profile

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

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

The assembly lines use the Tivoli 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 Tivoli Directory Integrator environment.

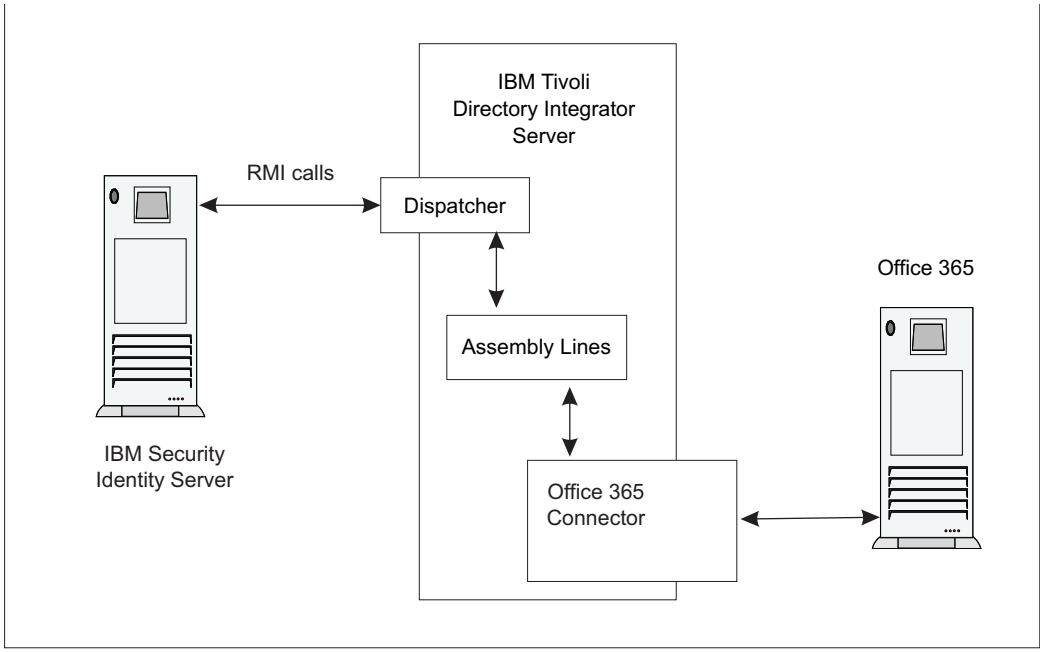

Figure 1. The architecture of the adapter

Supported configurations

The Office 365 Adapter supports a number of different configurations and is designed to operate with IBM Security Identity Governance and Intelligence.

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

- An IBM Security Identity server
- An IBM Tivoli 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 Tivoli Directory Integrator server.

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

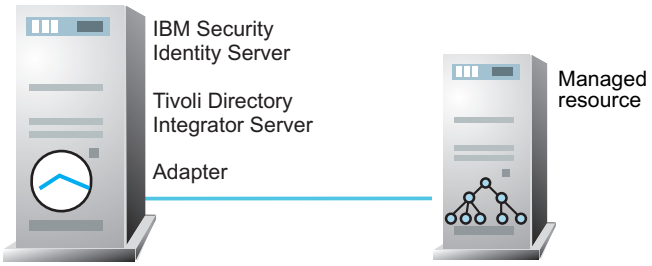

Figure 2. Single server configuration

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 Tivoli Directory Integrator based adapters, for IBM Security Identity Governance and Intelligence

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 Identity Governance and Intelligence 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 IBM Security 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 Tivoli Directory Integrator server.

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Operating system	The Office 365 Adapter can be used on any operating system that is supported by Tivoli 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	• IBM Tivoli 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 Tivoli 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.
IBM Security Identity server	The following servers are supported: • IBM Security Identity Manager server Version 6.0 • IBM Security Identity Manager server Version 7.0 • IBM Security Privileged Identity Manager Version 2.0 • IBM Security Identity Governance and Intelligence server Version 5.2.2
Dispatcher	Obtain the dispatcher installer from the IBM Passport Advantage website.
Tivoli Directory Integrator adapters solution directory	A Tivoli Directory Integrator adapters solution directory is a Tivoli 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.

For information about the prerequisites and supported operating systems for Tivoli Directory Integrator, see the *IBM Tivoli 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 Identity server 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 2. 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.	
Tivoli 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 Tivoli Directory Integrator is automatically installed with your IBM Security Identity Governance and Intelligence product, the default directory path for Tivoli 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 Tivoli 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 Tivoli Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Tivoli 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 Tivoli 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 Tivoli 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.

   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*.

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 IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Before you begin

- The IBM Security Identity Governance and Intelligence server is installed and running.
- You have root or administrator authority on the IBM Security Identity Governance and Intelligence 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.

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

Procedure

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

What to do next

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

Attribute mapping

Attribute mapping is required to define which target attributes correspond to the Identity Governance and Intelligence 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 Identity Governance and Intelligence 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 Identity Governance and Intelligence 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 Target Administration module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Identity Governance and Intelligence 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 management Portal. For details of the application registration process, see the Office 365 Community Blog web site.
2. 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 IBM Security Identity server, create a service/target so that IBM Security Identity server can communicate with the managed resource.

Before you begin

Complete “Importing the adapter profile” on page 11.

About this task

You must create an administrative user account for the adapter on the managed resource. Provide the account information when you create a target. 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.

Use the target form to provide information for the target. The actual target form fields might vary depending on whether the service form is customized. The target name and description that you provide for each target are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. On the Appliance Dashboard, select Identity Governance and IntelligenceAdministration Console from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration console is displayed.
3. From the navigation tree, click **Manage Targets**. The Select a Target page is displayed.
4. On the Select a Target page, click **Create**. The Create a Target wizard is displayed.
5. On the Select the Type of Target page, select a target type and 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 General Information page, specify the values for the target instance. The content of the General Information page depends on the type of target that you are creating. The creation of some targets might require more steps. It is specific to the profile (adapter). See the adapter's *Installation and Configuration Guide* for the more information.
7. On the Users and Groups page, which is displayed only for LDAP targets, complete the required fields.
8. On the Authentication page, which does not display for every target type, complete the required fields.
9. On the Dispatcher Attributes page, specify information about the dispatcher attributes and click **Next** or **OK**. The Dispatcher Attributes page is displayed only for IBM Security Directory Integrator based targets.
10. On the Status and Information page, view information about the adapter and managed resource and click **Next** or **Finish**. The adapter must be running to obtain the information.
11. On the Application Information page, type a name and description for the application, and then click **Finish**.
12. Optional: 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 target instance for a specific target 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 IBM Security 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.

Tivoli Directory Integrator location

Specify the URL for the IBM Tivoli Directory Integrator instance. The valid syntax for the URL is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the IBM Tivoli 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 3. 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 IBM Security 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 IBM Security Identity server.

TDI version
Specifies the version of the Tivoli 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.

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 IBM Security Identity server.
2. Run a full reconciliation from the IBM Security 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?

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 4. 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.

Chapter 5. Uninstalling

To remove an adapter from the IBM Security Identity server for any reason, you must remove all the components that were added during installation. Uninstalling an IBM Tivoli Directory Integrator based adapter mainly involves removing the connector file, and the adapter profile from the IBM Security 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 IBM Security Identity server. Before you delete the adapter profile, ensure that no objects exist on the IBM Security Identity server that reference the adapter profile.

Objects on the IBM Security 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 Tivoli 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 Identity Governance and Intelligence 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 IBM Security Identity servercommunicates 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 5. Supported user attributes

IBM Security Identity Governance and Intelligence name	**Attribute name in schema**	**Data type**
User ID	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
Set User Location	ero365location	String
Assign Licenses	ero365licvalue	String
Alternate Email Address	ero365othermail	String

Table 5. Supported user attributes (continued)

IBM Security Identity Governance and Intelligence name	Attribute name in schema	Data type
Group Membership	ero365groupoid	String
Administrator Role Membership	ero365roleoid	String

Group attributes

Table 6. Supported group attributes

IBM Security Identity Governance and Intelligence 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 Identity Governance and Intelligence **erGroupId**. You cannot use the adapter to modify this attribute.
- The **Group Name** attribute is mapped to the IBM Security Identity Governance and Intelligence **erGroupName** attribute. You cannot user the adapter to modify this attribute.

Object classes

Table 7. 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 Tivoli Directory Integrator configuration properties for the operation of the Office 365 Adapter, see the *Dispatcher Installation and Configuration Guide*.

Index

Printed in USA