IBM Security Identity Manager
Version 6.0

Microsoft Office 365 Adapter Installation and Configuration Guide

SC27-5686-00

IBM Security Identity Manager
Version 6.0

Microsoft Office 365 Adapter Installation and Configuration Guide

SC27-5686-00

Contents

Figures

Tables

Preface

About this publication

The *Office 365 Adapter Installation and Configuration Guide* provides the basic information to install and configure the IBM® Security Identity Manager Office 365 Adapter.

IBM Security Identity Manager was known previously as Tivoli® Identity Manager. The adapter enables connectivity between the IBM Security Identity Manager server and Office 365 applications.

Access to publications and terminology

This section provides:

- A list of publications in the "IBM Security Identity Manager library."
- Links to "Online publications."
- A link to the "IBM Terminology website."

IBM Security Identity Manager library

For a complete listing of the IBM Security Identity Manager and IBM Security Identity Manager Adapter documentation, see the online library (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm).

Online publications

IBM posts product publications when the product is released and when the publications are updated at the following locations:

IBM Security Identity Manager library
The product documentation site (http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.isim.doc_6.0/ic-homepage.htm) displays the welcome page and navigation for the library.

IBM Security Systems Documentation Central
IBM Security Systems Documentation Central provides an alphabetical list of all IBM Security Systems product libraries and links to the online documentation for specific versions of each product.

IBM Publications Center
The IBM Publications Center site (http://www-05.ibm.com/e-business/linkweb/publications/servlet/pbi.wss) offers customized search functions to help you find all the IBM publications you need.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at http://www.ibm.com/software/globalization/terminology.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at http://www.ibm.com/software/tivoli/education.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at http://www.ibm.com/software/support/probsub.html.

Appendix C, "Support information," on page 29 provides details about:

- What information to collect before contacting IBM Support.
- The various methods for contacting IBM Support.
- How to use IBM Support Assistant.
- Instructions and problem-determination resources to isolate and fix the problem yourself.

Note: The **Community and Support** tab on the product information center can provide additional support resources.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Chapter 1. Overview of the adapter

An adapter is a program that provides an interface between a managed resource and the IBM Security Identity Manager server. Adapters might or might not be on the managed resource, and the IBM Security Identity Manager 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 Manager 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

You must install several components for the adapter to function correctly.

The adapter requires the following components:

- The Dispatcher
- The IBM Tivoli Directory Integrator connector
- The IBM Security Identity Manager 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 IBM Security Identity Manager 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.

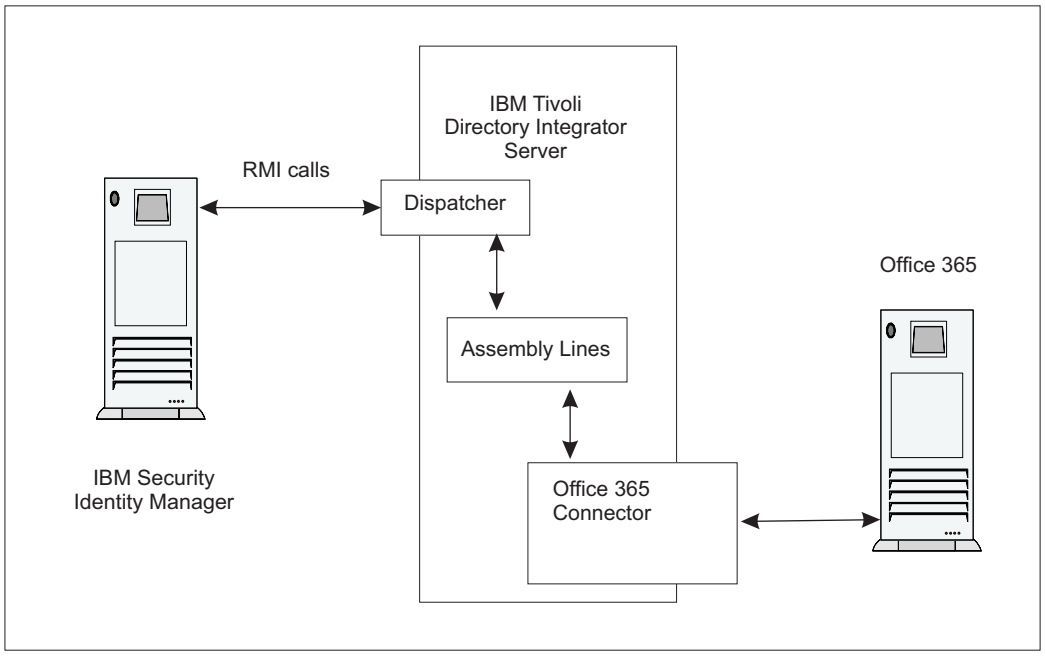

Figure 1. The architecture of the adapter

Supported configurations

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

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

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

As part of each configuration, the IBM Security Identity Manager 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 Manager server, IBM Tivoli Directory Integrator server, and the Office 365 Adapter on one server. That server communicates with the Office 365 domain.

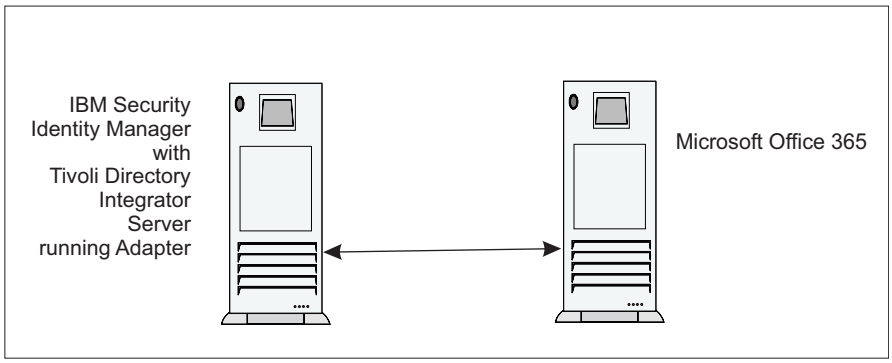

Figure 2. Single server configuration

Chapter 2. Adapter installation planning

Installing and configuring the adapter involves several steps that you must complete in the appropriate sequence. Review the roadmaps before you begin the installation process.

Preinstallation roadmap

Before you install the adapter, you must prepare the environment.

Perform the tasks that are listed in the following table.

Table 1. Preinstallation roadmap

Task	For more information
Obtain the installation software.	Download the software from Passport Advantage® website. See "Software download" on page 7.
Verify that your environment meets the software and hardware requirements for the adapter.	See "Prerequisites" on page 6.
Obtain and install the Dispatcher.	Download the software from Passport Advantage website. See "Software download" on page 7. Follow the installation instructions in the dispatcher download package.
Obtain the necessary information for the installation and configuration.	See "Installation worksheet for the adapter" on page 7.

Installation roadmap

For a new installation of the adapter, you must complete the necessary steps to install the adapter. These steps include post-installation configuration tasks and verifying the installation.

To install the adapter, complete the tasks that are listed in the following table:

Table 2. Installation roadmap

Task	For more information
Verify the Dispatcher installation.	See "Dispatcher installation verification" on page 9.
Configure the Apache HttpComponent HttpClient Java Library	See "Configuring the Apache HttpComponent HttpClient Java Library" on page 9.
Install the adapter.	See "Installing the adapter" on page 9.
Configure the SSL connection between the Dispatcher and the Office 365 service.	See "Configuring the SSL connection between the Dispatcher and the Office 365 domain" on page 10.
Import the adapter profile.	See "Importing the adapter profile into the IBM Security Identity Manager server" on page 11.

Table 2. Installation roadmap (continued)

Task	For more information
Verify the profile installation.	See "Adapter profile installation verification" on page 12.
Create an adapter user account.	See "Adapter user account creation" on page 12.
Obtain an Application Id and Secret key for the adapter.	See "Obtaining an Application Id and Secret key for the Office 365 Adapter" on page 13
Create a service.	See "Creating a service" on page 13.

Prerequisites

Verify that your environment meets all the prerequisites before you install the adapter.

The following table identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the Tivoli 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 Tivoli Directory Integrator.
Network Connectivity	Internet Protocol network
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
IBM Tivoli Directory Integrator	Version 7.1.1
IBM Security Identity Manager server	Version 6.0
IBM Security Identity Manager Dispatcher	Obtain the dispatcher installer from the IBM Passport Advantage website. See Table 1 on page 5
Tivoli Directory Integrator adapters solution directory	A Tivoli Directory Integrator adapters solution directory is a Tivoli Directory Integrator work directory for IBM Security Identity Manager 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: Administrator Guide*.

Software download

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

Go to IBM Passport Advantage.

See the *IBM Security Identity Manager Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet for the adapter

The worksheet identifies the information that you need before installing the adapter.

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.	
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 Manager 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. Adapter installation

All the 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 there is an upgrade to the Dispatcher. See "Dispatcher installation verification."

Dispatcher installation verification

If this installation is the first Tivoli Directory Integrator based adapter installation, you must install the Dispatcher before you install the adapter.

Install the Dispatcher on the same Tivoli Directory Integrator server where you want to install the adapter.

Obtain the dispatcher installer from the IBM Passport Advantage website, http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm. For information about Dispatcher installation, see the *Dispatcher Installation and Configuration Guide*.

Configuring the Apache HttpComponent HttpClient Java Library

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 into *ITDI_HOME*\jvm\jre\lib\ext 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*.

Installing the adapter

You must install the connector to establish communication between the adapter and the Dispatcher.

Before you begin

Do the following tasks:

- Verify that your site meets all the prerequisite requirements. See "Prerequisites" on page 6.
- Obtain a copy of the adapter software. See "Software download" on page 7.
- Obtain system administrator authority.

About this task

The adapter uses the Tivoli Directory Integrator Office 365 connector. The connector is not available with the base Tivoli Directory Integrator product.

The adapter installation involves the Tivoli Directory Integrator Office 365 connector installation. Before you install the adapter, make sure that the Dispatcher is installed. See "Dispatcher installation verification" on page 9.

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 Dispatcher service.

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. Take one of the following actions:
   - If the Dispatcher already has a configured keystore, use the **keytool.exe** program to import the **MSIT Machine Auth CA 2** certificate.
   - If the keystore is not configured, create it by running the following command from a command prompt. Type the command on a single line.

     ```
     keytool -import -alias O365 -file c:\MSITMachineAuthCA2.crt
     -keystore c:\truststore.jks -storepass passw0rd
     ```
8. Edit *ITDI_HOME*/timsol/solution.properties file to specify truststore and keystore information. In the current release, only **jks-type** is supported:

   ```
   # Keystore file information for the server authentication.
   # It is used to verify the server's public key.
   # example
   javax.net.ssl.trustStore=truststore.jks
   javax.net.ssl.trustStorePassword=passw0rd
   javax.net.ssl.trustStoreclass=jks
   ```

   Note: If these key properties are not configured yet, you can set **truststore** to the same value that contains the Office 365 certificate. Otherwise, you must import the **MSIT Machine Auth CA 2** certificate to the truststore specified in javax.net.ssl.trustStore.
9. After you modify the solution.properties file, restart the Dispatcher. For information about SSL configuration, see the *Dispatcher Installation and Configuration Guide*.

Importing the adapter profile into the IBM Security Identity Manager server

An adapter profile defines the types of resources that the IBM Security Identity Manager server can manage.

Before you begin

Before you begin to import the adapter profile, verify that the following conditions are met:

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

About this task

The IBM Security Identity Manager server must have the adapter profile before you can add the adapter as a service. The server uses the profile to recognize the adapter. The adapter service establishes communication between IBM Security Identity Manager, the adapter, and the managed resource. You can import the adapter profile by using the Import feature of IBM Security Identity Manager.

The files that are packaged with the adapter include the Office365Profile.jar file. The Office365Profile.jar file includes all the files that are required to define the adapter schema, account form, service form, and profile properties.

Procedure

1. Log on to the IBM Security Identity Manager server by using an account that has the authority to perform administrative tasks.
2. In the My Work pane, expand **Configure System** and click **Manage Service Types**.
3. On the Manage Service Types page, click **Import** to display the Import Service Types page.
4. Specify the location of the `Office365Profile.jar` file in the **Service Definition File** field by doing one of the following tasks:
   - Type the complete location of where the file is stored.
   - Use **Browse** to navigate to the file.
5. Click **OK**.

What to do next

- When you import the adapter profile and if you receive an error that is related to the schema, see the `trace.log` file for information about the error. The `trace.log` file location is specified by using the **`handler.file.fileDir`** property that is defined in the IBM Security Identity Manager `enRoleLogging.properties` file. The `enRoleLogging.properties` file is installed in the IBM Security Identity Manager `\data` directory.
- Restart the IBM Security Identity Manager for the change to take effect.
- If you are upgrading the adapter, restart the Dispatcher service.

Adapter profile installation verification

After you install the adapter profile, verify that the installation was successful.

An unsuccessful installation:

- Might cause the adapter to function incorrectly.
- Prevents you from creating a service with the adapter profile.

To verify that the adapter profile is successfully installed:

- Create a service with the adapter profile. For more information about creating a service, see "Creating a service" on page 13.
- Open an account on the service.

If you are unable to create a service with the adapter profile or open an account on the service, the adapter profile is not installed correctly. You must import the adapter profile again.

Adapter user account creation

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

For information about creating an administrative account, see the documentation for your managed resource.

For information about creating a service, see "Creating a service" on page 13.

Ensure that the account has sufficient privileges to administer the Office 365 users.

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 a service

You must create a service for the adapter before the IBM Security Identity Manager server can use the adapter to communicate with the managed resource.

About this task

To create or change a service, you must use the service form to provide information for the service. The actual service form fields might vary depending on whether the service form is customized.

Procedure

1. Log on to the IBM Security Identity Manager server with an account that has the authority to do administrative tasks.
2. In the My Work pane, click **Manage Services** and click **Create**.
3. On the Select the Type of Service page, select **Office 365 Profile Service**.
4. Click **Next** to display the adapter service form.
5. Complete the following fields on the service form:

Adapter Details

Service Name
Specify a name that defines the adapter service on the IBM Security Identity Manager 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 Tivoli Directory Integrator instance. The valid syntax for the URL is `rmi://ip-address:port/ITDIDispatcher`, where *ip-address* is the Tivoli Directory Integrator host and *port* is the port number for the Dispatcher. The default URL is

`rmi://localhost:1099/ITDIDispatcher`

For information about changing the port number, see the *Dispatcher Installation and Configuration Guide*.

Owner
Specify an IBM Security Identity Manager 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 an IBM Security Identity Manager 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.

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 IBM Security Identity Manager. 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 IBM Security Identity Manager 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 Manager 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 IBM Security Identity Manager test request was sent successfully to the adapter.
- Verify the adapter configuration information.

- Verify IBM Security Identity Manager 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.

6. Click **Finish**.

Language pack installation

The adapters use the same language package as IBM Security Identity Manager.

See the IBM Security Identity Manager library and search for information about installing language packs.

Chapter 4. Verifying that the adapter is working correctly

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

Procedure

1. Test the connection for the service that you created on IBM Security Identity Manager.
2. Run a full reconciliation from IBM Security Identity Manager.
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 IBM Security Identity Manager log file `trace.log` to ensure that no errors are reported when you run an adapter operation.

Chapter 5. Adapter error troubleshooting

Troubleshooting can help you determine why a product does not function properly.

Troubleshooting topics provide information and techniques for identifying and resolving problems with the adapter. It also provides information about known issues and limitations that exist.

Techniques for troubleshooting problems

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. 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 know where to start to 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 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 platform or operating system, or is it common across multiple platforms or 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 were 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 must look only as far as 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?
- Does a certain sequence of events happen when the problem occurs?
- 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. 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?
- Are there multiple users or applications that are encountering the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

For information about obtaining support, see Appendix C, "Support information," on page 29.

Runtime problems

During the operation of IBM Security Identity Manager with Office 365 Adapter, you might encounter errors. Use this information and the information that is provided by the message to resolve the error.

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

Table 5. 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 6. Adapter uninstallation

To completely uninstall the Office 365 Adapter, you must do two procedures:

1. Uninstall the adapter connector from Tivoli Directory Integrator server.
2. Remove the adapter profile from the IBM Security Identity Manager server.

Uninstalling the adapter from the Tivoli Directory Integrator server

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*\jvm\jre\lib\ext directory.

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

4. Start the Dispatcher service.

Adapter profile: Removal from the IBM Security Identity Manager server

Before you remove the adapter profile, ensure that no objects exist on your IBM Security Identity Manager server that reference the adapter profile.

These objects are examples of objects on the IBM Security Identity Manager 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 for the Office 365 Adapter, do not uninstall the Dispatcher.

For specific information about how to remove the adapter profile, see the online help or the IBM Security Identity Manager product documentation.

Appendix A. Adapter attributes, object classes, and configuration properties

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 6. Supported user attributes

IBM Security Identity Manager 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
Group Membership	ero365groupoid	String
Administrator Role Membership	ero365roleoid	String

Group attributes

Table 7. Supported group attributes

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

Object classes

Table 8. 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*.

Appendix B. Conventions used in this publication

This publication uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This publication uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations**:)
- Keywords and parameters in text

Italic

- Citations (examples: titles of publications, diskettes, and CDs
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Operating system-dependent variables and paths

This guide uses the Windows convention for specifying environment variables and for directory notation.

When using the Unix command line, replace %variable% with $variable for environment variables and replace each backslash (\) with a forward slash (/) in directory paths. The names of environment variables are not always the same in Windows and UNIX. For example, %TEMP% in the Windows operating system is equivalent to $tmp in a UNIX operating system.

Note: If you are using the bash shell on a Windows system, you can use the UNIX conventions.

Appendix C. Support information

You have several options to obtain support for IBM products.

Searching knowledge bases

You can often find solutions to problems by searching IBM knowledge bases. You can optimize your results by using available resources, support tools, and search methods.

About this task

You can find useful information by searching the product documentation for IBM Security Identity Manager. However, sometimes you must look beyond the product documentation to answer your questions or resolve problems.

Procedure

To search knowledge bases for information that you need, use one or more of the following approaches:

1. Search for content by using the IBM Support Assistant (ISA).

   ISA is a no-charge software serviceability workbench that helps you answer questions and resolve problems with IBM software products. You can find instructions for downloading and installing ISA on the ISA website.
2. Find the content that you need by using the IBM Support Portal.

   The IBM Support Portal is a unified, centralized view of all technical support tools and information for all IBM systems, software, and services. The IBM Support Portal lets you access the IBM electronic support portfolio from one place. You can tailor the pages to focus on the information and resources that you need for problem prevention and faster problem resolution. Familiarize yourself with the IBM Support Portal by viewing the demo videos (https://www.ibm.com/blogs/SPNA/entry/the_ibm_support_portal_videos) about this tool. These videos introduce you to the IBM Support Portal, explore troubleshooting and other resources, and demonstrate how you can tailor the page by moving, adding, and deleting portlets.
3. Search for content about IBM Security Identity Manager by using one of the following additional technical resources:
   - IBM Security Identity Manager version 6.0 technotes and APARs (problem reports).
   - IBM Security Identity Manager Support website.
   - IBM Redbooks®.
   - IBM support communities (forums and newsgroups).
4. Search for content by using the IBM masthead search. You can use the IBM masthead search by typing your search string into the Search field at the top of any ibm.com® page.
5. Search for content by using any external search engine, such as Google, Yahoo, or Bing. If you use an external search engine, your results are more likely to

include information that is outside the ibm.com domain. However, sometimes you can find useful problem-solving information about IBM products in newsgroups, forums, and blogs that are not on ibm.com.

Tip: Include "IBM" and the name of the product in your search if you are looking for information about an IBM product.

Obtaining a product fix

A product fix might be available to resolve your problem.

About this task

You can get fixes by following these steps:

Procedure

1. Obtain the tools that are required to get the fix. You can obtain product fixes from the *Fix Central Site*. See http://www.ibm.com/support/fixcentral/.
2. Determine which fix you need.
3. Download the fix. Open the download document and follow the link in the "Download package" section.
4. Apply the fix. Follow the instructions in the "Installation Instructions" section of the download document.

Contacting IBM Support

IBM Support assists you with product defects, answers FAQs, and helps users resolve problems with the product.

Before you begin

After trying to find your answer or solution by using other self-help options such as technotes, you can contact IBM Support. Before contacting IBM Support, your company or organization must have an active IBM software subscription and support contract, and you must be authorized to submit problems to IBM. For information about the types of available support, see the Support portfolio topic in the "*Software Support Handbook*".

Procedure

To contact IBM Support about a problem:

1. Define the problem, gather background information, and determine the severity of the problem. For more information, see the Getting IBM support topic in the *Software Support Handbook*.
2. Gather diagnostic information.
3. Submit the problem to IBM Support in one of the following ways:
   - Using IBM Support Assistant (ISA):

     Any data that has been collected can be attached to the service request. Using ISA in this way can expedite the analysis and reduce the time to resolution.

     a. Download and install the ISA tool from the ISA website. See http://www.ibm.com/software/support/isa/.
     b. Open ISA.

c. Click **Collection and Send Data**.
d. Click the **Service Requests** tab.
e. Click **Open a New Service Request**.

- Online through the IBM Support Portal: You can open, update, and view all of your service requests from the Service Request portlet on the Service Request page.
- By telephone for critical, system down, or severity 1 issues: For the telephone number to call in your region, see the Directory of worldwide contacts web page.

Results

If the problem that you submit is for a software defect or for missing or inaccurate documentation, IBM Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the IBM Support website daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix D. Accessibility features for IBM Security Identity Manager

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

Accessibility features

The following list includes the major accessibility features in IBM Security Identity Manager.

- Support for the Freedom Scientific JAWS screen reader application
- Keyboard-only operation
- Interfaces that are commonly used by screen readers
- Keys that are discernible by touch but do not activate just by touching them
- Industry-standard devices for ports and connectors
- The attachment of alternative input and output devices

The IBM Security Identity Manager library, and its related publications, are accessible.

Keyboard navigation

This product uses standard Microsoft Windows navigation keys.

Related accessibility information

The following keyboard navigation and accessibility features are available in the form designer:

- You can use the tab keys and arrow keys to move between the user interface controls.
- You can use the Home, End, Page Up, and Page Down keys for more navigation.
- You can launch any applet, such as the form designer applet, in a separate window to enable the Alt+Tab keystroke to toggle between that applet and the web interface, and also to use more screen workspace. To launch the window, click **Launch as a separate window**.
- You can change the appearance of applets such as the form designer by using themes, which provide high contrast color schemes that help users with vision impairments to differentiate between controls.

IBM and accessibility

See the IBM Human Ability and Accessibility Center For more information about the commitment that IBM has to accessibility.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features contained in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM might have patents or pending patent applications that cover subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it to enable: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information might be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments might vary significantly. Some measurements might have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements might have been estimated through extrapolation. Actual results might vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements, or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding the future direction or intent of IBM are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to

IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations might not appear.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both: http://www.ibm.com/legal/copytrade.shtml

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

The Oracle Outside In Technology included herein is subject to a restricted use license and can only be used in conjunction with this application.

Index

Printed in USA

SC27-5686-00