

IBM Security Verify Governance
10.0

*Google Workspace Adapter Installation
and Configuration Guide*



Contents

- Figures..... V**
- Tables..... vii**
- Chapter 1. Overview..... 1**
 - Features of the adapter.....1
 - Architecture of the adapter.....1
 - Supported configurations..... 2
- Chapter 2. Planning..... 3**
 - Roadmap..... 3
 - Prerequisites..... 4
 - Software downloads..... 5
 - Installation worksheet..... 6
- Chapter 3. Installing..... 7**
 - Installing the dispatcher.....7
 - Installing the adapter binaries or connector.....7
 - Installing 3rd party client libraries..... 7
 - Creating a Service Account in Google Workspace..... 9
 - Delegating domain-wide authority to the service account..... 9
 - Configuring the SSL connection between the Dispatcher and the Google Workspace server..... 10
 - Restarting the adapter service..... 11
 - Importing the adapter profile..... 11
 - Importing attribute mapping file..... 12
 - Adding a connector..... 13
 - Enabling connectors..... 14
 - Reviewing and setting channel modes for each new connector..... 15
 - Attribute Mapping..... 16
 - Service/Target form details..... 17
 - Installing the ILMT tags..... 19
 - Verifying that the adapter is working correctly..... 19
- Chapter 4. Configuring..... 21**
 - Customized attributes..... 21
 - Schema extensions and custom attributes.....21
 - Copying the GoogleAppsProfile.jar file and extracting files..... 21
 - Modifying the assembly lines..... 22
 - Updating the schema.dsm1 file..... 24
 - Modifying the CustomLabels.properties file..... 24
 - Adapter form modification (optional)..... 25
 - Editing Google Workspace Adapter profiles on the UNIX or Linux operating system..... 25
 - Creating a JAR file and importing the profile..... 25
 - Create a GoogleAppsCustomAttr.txt file with custom attributes..... 26**
 - Verifying that the adapter is working correctly..... 26
- Chapter 5. Upgrading..... 27**
 - Upgrading the adapter binaries or connector..... 27
 - Upgrading the adapter profile..... 27

| | |
|--|-----------|
| Upgrading the Google Directory API Java Client Library..... | 27 |
| Chapter 6. Troubleshooting..... | 29 |
| Techniques for troubleshooting problems..... | 29 |
| Error messages and problem solving..... | 30 |
| Chapter 7. Uninstalling..... | 33 |
| Removing the adapter binaries or connector..... | 33 |
| Deleting the adapter profile..... | 33 |
| Chapter 8. Reference..... | 35 |
| Adapter attributes and object classes..... | 35 |
| Index..... | 37 |

Figures

- 1. The architecture of the Google Workspace Adapter..... 2
- 2. Single server configuration.....2

Tables

| | |
|---|----|
| 1. Prerequisites to install the adapter..... | 4 |
| 2. Required information to install the adapter..... | 6 |
| 3. Prerequisites for enabling a connector..... | 14 |
| 4. Ports..... | 17 |
| 5. Runtime problems..... | 31 |
| 6. Supported user attributes..... | 35 |
| 7. Supported group attributes..... | 36 |
| 8. Supported object classes..... | 36 |

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server.

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

The Google Workspace Adapter uses the Security Directory Integrator functions to facilitate communication between the Identity server and Google Workspace.

Features of the adapter

This adapter automates several administrative tasks on the Google Workspace server.

You can use the adapter to automate the following tasks:

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

Architecture of the adapter

Several components are involved in running and using the adapter. Install all these components so that the adapter can function correctly.

The adapter requires the following components:

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

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

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

The assembly lines use the Security Directory Integrator components to undertake user management-related tasks on the Google Workspace domain. They perform these tasks remotely by using the ID and password of a user that has administrator privileges.

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

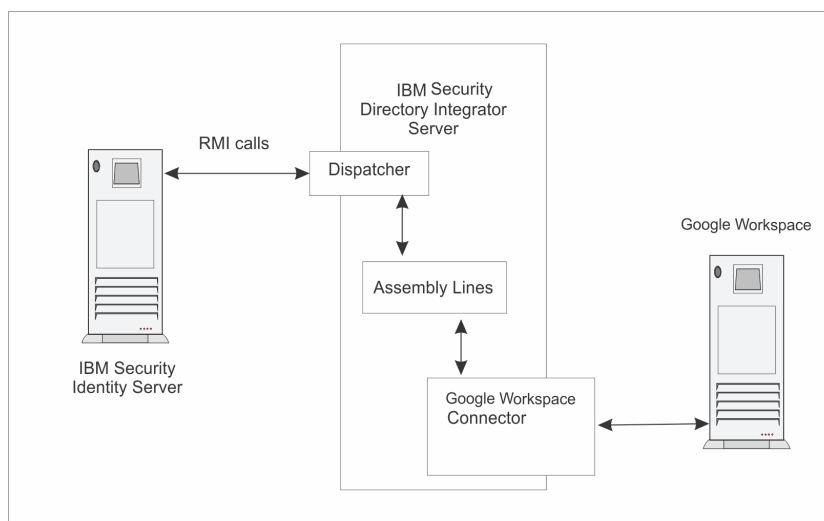


Figure 1. The architecture of the Google Workspace Adapter

Supported configurations

The Google Workspace Adapter supports a number of different configurations and is designed to operate with IBM Security Verify Governance.

The following components are the fundamental components of a Google Workspace Adapter environment:

- An Identity server
- An IBM Security Directory Integrator server
- The Google Workspace Adapter

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

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

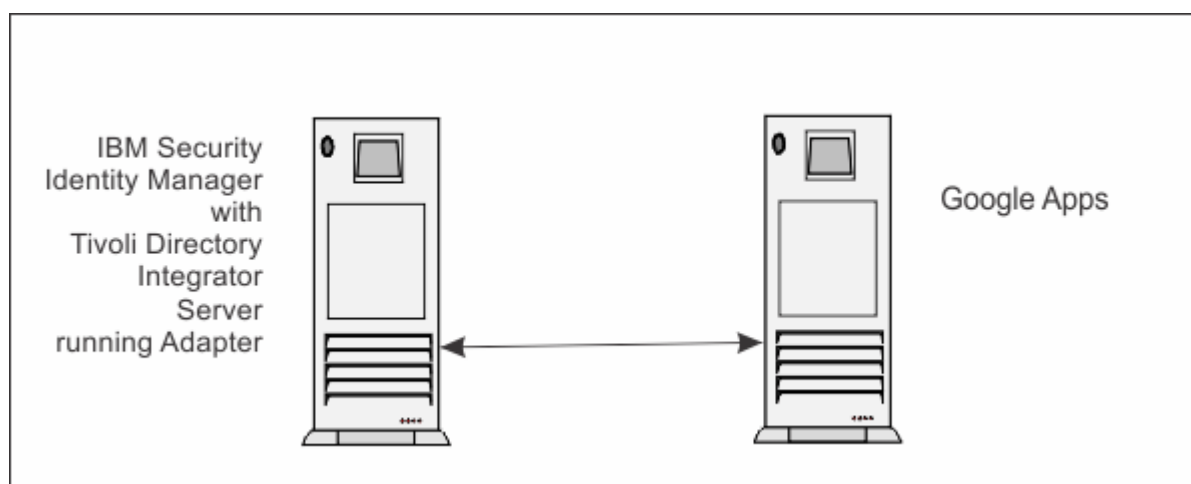


Figure 2. Single server configuration

Chapter 2. Planning

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

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the Identity server and the adapter.
 - a. Configure 1-way authentication.
 - b. Configure 2-way authentication.
2. Configure secure communication between the adapter and the managed target.
 - a. Configure 1-way authentication.

- b. Configure 2-way authentication.
- 3. Configure the adapter.
- 4. Modify the adapter profiles.
- 5. Customize the adapter.

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Prerequisites

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

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 Security Directory Integrator server.

| <i>Table 1. Prerequisites to install the adapter</i> | |
|--|--|
| Prerequisite | Description |
| Operating system | The Google Workspace Adapter can be used on any operating system that is supported by Security Directory Integrator. |
| Network Connectivity | Internet Protocol network |
| System Administrator authority | To complete the adapter installation procedure, you must have system administrator authority. |

Table 1. Prerequisites to install the adapter (continued)

| Prerequisite | Description |
|---|--|
| Directory Integrator | <ul style="list-style-type: none"> IBM® Security Directory Integrator 7.2 + FP6 + 7.2.0-ISS-SDI-LA0019 <p>Note:</p> <ul style="list-style-type: none"> Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2. |
| Identity server | <p>The following servers are supported:</p> <ul style="list-style-type: none"> IBM Security Identity Manager server Version 6.0 IBM Security Identity Manager server Version 7.0 IBM Security Identity Governance v5.2.x IBM Security Verify Governance Identity Manager v10.0.x IBM Security Verify Governance v10.0.x |
| Security Directory Integrator adapters solution directory | <p>A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters.</p> <p>For more information, see the <i>Dispatcher Installation and Configuration Guide</i>.</p> |
| Google Workspace | <ul style="list-style-type: none"> Premier edition Education edition Partner edition |
| Google Data Java Client Library | <p>See the <i>Google Workspace Adapter Release Notes</i> for the supported API package name and version.</p> |

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1: Administrator Guide*.

Software downloads

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

Go to [IBM Passport Advantage](#).

See the corresponding *IBM Security Verify Governance 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.

| <i>Table 2. Required information to install the adapter</i> | | |
|---|---|--|
| Required information | Description | Value |
| Administrator account ID and password | An administrator account ID and password on the managed resource that has administrative rights for running the Google Workspace Adapter. | |
| Security Directory Integrator Home Directory | The <i>ITDI_HOME</i> directory contains the <i>jars/connectors</i> subdirectory that contains adapter JAR files. For example, the <i>jars/connectors</i> subdirectory contains the JAR file for the UNIX adapter. | <p>If Security Directory Integrator is automatically installed with your IBM Security Verify Governance product, the default directory path for Security Directory Integrator is as follows:</p> <p>Windows:</p> <ul style="list-style-type: none"> for version 7.1: <i>drive\Program Files\IBM\TDI\V7.1</i> <p>UNIX:</p> <ul style="list-style-type: none"> for version 7.1: <i>/opt/IBM/TDI/V7.1</i> |
| Adapters solution directory | When you install the dispatcher, the installer prompts you to specify a file path for the solution directory. For more information about the solution directory, see the <i>Dispatcher Installation and Configuration Guide</i> . | <p>The default solution directory is at:</p> <p>Windows:</p> <ul style="list-style-type: none"> for version 7.1: <i>drive\Program Files\IBM\TDI\V7.1\tim sol</i> <p>UNIX:</p> <ul style="list-style-type: none"> for version 7.1: <i>/opt/IBM/TDI/V7.1/timsol</i> |

Chapter 3. Installing

Installing the adapter mainly involves importing the adapter profile and creating an adapter service. Depending on the adapter, several other tasks can be involved to completely install it.

All IBM Security Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See [Dispatcher Installation Verification](#).

Installing the dispatcher

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

If you already installed the RMI Dispatcher for another adapter, you do not need to reinstall it.

If you have not yet installed the RMI Dispatcher in the Security Directory Integrator environment, download the Dispatcher installer from the [IBM Passport Advantage](#) website. For more information about the installation, see the *Dispatcher Installation and Configuration Guide*.

Installing the adapter binaries or connector

The connector might or might not be available with the base Security Directory Integrator or Security Directory Integrator product. The connector is required to establish communication between the adapter and the Dispatcher.

Before you begin

- The Dispatcher must be installed.

Procedure

1. Create a temporary directory on the workstation where you want to extract the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `GoogleAppsConnector.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 Google Directory API Java Client Library at run time.

Before you begin

The API library must be downloaded from the [Google Developers website](https://developers.google.com/admin-sdk/directory/v1/libraries) (<https://developers.google.com/admin-sdk/directory/v1/libraries>).

About this task

Google might provide client library files, which are newer than what is documented in the guide or in the release notes. While the newer library files can work with the adapter, use these files with caution because they are not tested by IBM. If possible, use the same version as listed here or in the release notes.

Procedure

1. Go to the [Google Developers website](https://developers.google.com/admin-sdk/directory/v1/libraries)(<https://developers.google.com/admin-sdk/directory/v1/libraries>) and search for the Google Directory API Java Client Library package that is listed in the *Google Workspace Adapter Release Notes*.
2. Download the Google Directory API Java Client Library package to a temporary directory.
3. Copy these files into `ITDI_HOME\jars\3rdparty\others` directory.
See the *Google Workspace Adapter Release Notes* for the path to these JAR files in the package.
 - `commons-logging-1.1.1.jar`: This jar file can be found at <https://mvnrepository.com/artifact/commons-logging/commons-logging/1.1.1>
 - `google-api-client-java6-1.25.0.jar`
 - `google-api-client-1.25.0.jar`
 - `google-api-services-admin-directory_v1-rev104-1.25.0.jar`
 - `google-http-client-1.25.0.jar`
 - `google-http-client-jackson2-1.25.0.jar`
 - `google-oauth-client-1.25.0.jar`
 - `google-oauth-client-java6-1.25.0.jar`
 - `google-oauth-client-jetty-1.25.0.jar`
 - `httpClient-4.5.5.jar`
 - `httpcore-4.0.1.jar`: This jar file can be found at <https://mvnrepository.com/artifact/org.apache.httpcomponents/httpcore/4.0.1>
 - `jackson-core-2.9.6.jar`
 - `jetty-6.1.26.jar`
 - `jetty-util-6.1.26.jar`
 - `guava-25.1-jre.jar`: This jar file can be found at: <https://mvnrepository.com/artifact/com.google.guava/guava>
 - `gson-2.8.5.jar`: This jar can be found at <https://mvnrepository.com/artifact/com.google.code.gson/gson>
4. Go to the [Google Developers website](https://search.maven.org/artifact/com.google.apis/google-api-services-groupsettings)<https://search.maven.org/artifact/com.google.apis/google-api-services-groupsettings>) and search for the Google Groups Settings API Java Client Library package.
5. Download the Google Groups Settings API Java Client Library package to a temporary directory.
6. Copy these files into `ITDI_HOME\jars\3rdparty\others` directory.
See the *Google Workspace Adapter Release Notes* for the path to these JAR files in the package.
 - `google-api-services-groupsettings-v1-rev75-1.25.0.jar`
7. Copy the latest version of the `commons-codec-1.11.jar` file to `ITDI_HOME\jars\3rdparty\IBM\axis2` directory.
The jar file can be found at <https://mvnrepository.com/artifact/commons-codec/commons-codec>.
8. Restart the Dispatcher service.
For information about starting and stopping the service, see the *Dispatcher Installation and Configuration Guide*.

Creating a Service Account in Google Workspace

To create a service for the Google Workspace Adapter, you specify the Google Workspace domain details. To populate those fields, you must create a service account in Google Workspace. The service account is not predefined before using the Google Workspace Adapter.

Procedure

1. Open the Google Cloud Console (<https://console.developers.google.com>).
2. Select a project. If there are no existing projects, create a project.
3. Enable the API.
 - a) On the navigation menu, select **API & Services > Library** option if it is not already selected.
 - b) In the displayed list of APIs, click **Admin SDK** and **Groups Settings API**. Enable these options if they are not already enabled.
4. On the navigation menu, select **Credentials**.
5. Optional: If there are no existing service accounts, create a service account.
 - a) To view existing Service Accounts, click **Manage service account**. The list of service accounts are displayed.

Note: Google might already have created accounts. Do **not** use those accounts.
 - b) To create a new service account click **Create Credentials**.
 - c) From the drop-down menu, select **Service Account Key**.
 - d) Enter the account name.

The ID is automatically populated.
 - e) To furnish a new private key, select the **p12** key type.
 - f) Click **Create**.

You are prompted to download the key.
6. Click **Create**. You are prompted to download the key.

Note: Take note of the **Service account ID** and **service account name**.
7. From Navigation Menu, select **IAM & admin > Service accounts**.
 - a) Select the service account that you have created from the list of all service accounts.
 - b) Click **Edit** and click **SHOW DOMAIN-WIDE DELEGATION**.
 - c) Enable the **G Suite Domain-wide Delegation** check box for the Service account.

Delegating domain-wide authority to the service account

To access user data in the Google Workspace domain, grant domain-wide authority to your service account.

About this task

You must have Administrator privileges on the Google Workspace domain.

Procedure

1. Open the Google Workspace domain administrative console (<http://admin.google.com/>).
2. Select **Security** from the list of controls. If you cannot view it, select **More controls > Security**.

Note: If you cannot see the controls, make sure you are signed in as an administrator for the domain.
3. Select **Show more > Advanced settings** from the list of options.
4. Select **Manage API client access** in the Authentication section.

5. In **Client name**, enter the service account Client ID. You can find your service account client ID in the Service accounts section of the **Developers Console's Permissions** page.
6. In **One or More API Scopes**, enter the list of scopes required by the adapter.

```
https://www.googleapis.com/auth/admin.directory.user,  
https://www.googleapis.com/auth/admin.directory.orgunit,  
https://www.googleapis.com/auth/admin.directory.group,  
https://www.googleapis.com/auth/admin.directory.user.alias,  
https://www.googleapis.com/auth/apps.groups.settings
```

7. Click **Authorize**.

Configuring the SSL connection between the Dispatcher and the Google Workspace server

To enable communication between the adapter and the Google Workspace server, 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://www.google.com/a/DOMAIN_NAME/`.
The *DOMAIN_NAME* is your Google Workspace Domain.
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 **CA Root** 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 IMS Server 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 googapps -file c:\GOOGLEAPPS.cer  
-keystore c:\truststore.jks -storepass passw0rd
```

8. Download the Base-64 encoded X.509 (.CER) format of the CA certificate Root 1 - Equifax Secure Certificate Authority. Go to the [GeoTrust](#) website and search for ca certificates.
9. Import the certificate into the keystore that was created in step 7.

```
keytool -import -alias equifax  
-file C:\Equifax_Secure_Certificate_Authority.cer  
-keystore C:\truststore.jks -storepass passw0rd
```

10. 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=password
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 Google Workspace certificate. Otherwise, you must import the IMS Server certificate to the truststore specified in `javax.net.ssl.trustStore`.

11. After you modify the `solution.properties` file, restart the Dispatcher.

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

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

Before you begin

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

About this task

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

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

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

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

Procedure

1. Log in to the Verify Governance Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.

3. Select **Manage > Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions > Import**.
6. On the **Import** page, complete these steps:
 - a) Select **Profile**.
 - b) Click **Browse** to locate the JAR file that you want to import.
 - c) Click **Upload file**.

A message indicates that you successfully imported a profile.
7. Click **Close**.

The new profile is displayed in the list of profiles.

Results

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

What to do next

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

- Import the attribute mapping file. See [“Importing attribute mapping file”](#) on page 12.
- Create a connector that uses the target profile. See [“Adding a connector”](#) on page 13.

Importing attribute mapping file

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

About this task

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

Procedure

1. Log in to the Verify Governance Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage > Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions > Import**.
6. On the **Import** page, complete these steps:
 - a) Select **Attribute Mapping**.
 - b) Click **Browse** to locate the attribute mapping file that you want to import.
 - c) Click **Upload file**.

A message indicates that you successfully imported the file.
7. Click **Close**.

Adding a connector

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

Before you begin

Complete [Importing the adapter profile](#).

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

About this task

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

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

Procedure

To add a connector, complete these steps.

1. Log in to the Verify Governance Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage > Connectors**.
A list of connectors is displayed on the **Connectors** tab.
4. Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Click **Actions > Add**.
The **Connector Details** pane is enabled for your input.
7. On the **Connector Details** tab, complete these steps:
 - a) Assign a name and description for the connector.
 - b) Select the target profile type as **Identity Brokerage** and its corresponding target profile.
 - c) Select the entity, such as **Account** or **User**.
Depending on the connector type, this field might be preselected.
 - d) Optional: Select **Trace ON** and the corresponding **Trace Level** to enable trace logs.
The available trace levels are DEBUG, INFO, and ERROR.
 - e) Optional: Select **History ON** to save and track the connector usage.
 - f) Click **Save**.
The fields for enabling the channels for sending and receiving data are now visible.
 - g) Select and set the connector properties in the **Global Config** accordion pane.
For information about the global configuration properties, see [Global Config accordion pane](#).
 - h) Click **Save**. The fields for enabling the channels for sending and receiving data are now visible.

Results

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

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

What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance. For more information, see [“Enabling connectors” on page 14](#).

Enabling connectors

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

Before you begin

| <i>Table 3. Prerequisites for enabling a connector</i> | |
|--|---|
| Prerequisite | Find more information |
| A connector must exist in Verify Governance. | “Adding a connector” on page 13 . |
| Ensure that you enabled the appropriate channel modes for the connector. | “Reviewing and setting channel modes for each new connector” on page 15 . |

Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage > Connectors**.
A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
 - a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

Enable write-to channel

Propagates every change in the Access Governance Core repository into the target system.

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

Enable read-from channel

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

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

Enable reconciliation

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

Results

The connector is enabled

What to do next

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

Reviewing and setting channel modes for each new connector

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

About this task

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

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

Procedure

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

1. Log in to the Verify Governance Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage > Connectors**.
A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
 - a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed, in which you can do more configuration, such as mapping attributes and setting up rules.
 - Enable write-to channel**
Propagates every change in the Access Governance Core repository into the target system.
 - Enable read-from channel**
Reads the INPUT EVENTS and USER DATA from the target system. Imports data from the target system to the Access Governance Core repository.
 - Enable reconciliation**
Synchronizes the modified data between the Access Governance Core repository and the target system.
8. Select **Monitor > Change Log Sync Status**.
A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
 - a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
 - b) Select a connector, and click **Actions > Sync Now**.
The synchronization process begins.
 - c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.
Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
11. When the connector configuration is complete, enable the connector by completing these steps:
 - a) Select **Manage > Connectors**.

b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.

c) Click **Save**.

For more information, see [“Enabling connectors” on page 14](#).

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

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

12. Start the connector by selecting **Monitor > Connector Status**. Select the connector that you want to start, and then select **Actions > Start**.

Attribute Mapping

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

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

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

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

| Attribute | Mapped Attribute |
|------------|------------------|
| eruid | CODE |
| erpassword | PASSWORD |

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

Service/Target form details

Complete the service/target form fields.

Adapter Details

Service Name

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

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

Description

Specify a description that identifies the service for your environment.

Security Directory Integrator location

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

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

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

| 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 Google Workspace service instance requires.

Google Workspace Domain Details**Primary Domain**

Name of the primary Google Workspace domain.

Secondary Domains

List of secondary Google Workspace domains; separated by comma (",").

Domain Admin Email

Specify the login email address of the Google Workspace Domain administrator.

Application Name

Application name of the adapter that is registered in Google Workspace.

Client Email

The Service account ID of the adapter's service account in Google Workspace.

Client Key Path

Location of the application's private key.

Proxy Server host

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

Proxy Server port

Specify the port number for the proxy server.

Enable TDI detailed debugging

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

Dispatcher Attributes**AL FileSystem Path**

Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from Identity server. You can specify a file path to load the assembly lines from the profiles directory of the Windows operating system such as: *drive:* \Program Files\IBM\TDI\V7.1\profiles. You can also 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/profiles

Max Connection Count

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

Disable AL Caching

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

Status and information

The page contains read only information about the adapter and managed resource. These fields are examples. The actual fields vary depending on the type of adapter and how the service form is configured. The adapter must be running to obtain the information. Click **Test Connection** to populate the fields.

Last status update: Date

Specifies the most recent date when the Status and information tab was updated.

Last status update: Time

Specifies the most recent time of the date when the Status and information tab was updated.

Managed resource status

Specifies the status of the managed resource that the adapter is connected to.

Adapter version

Specifies the version of the adapter that the service uses to provision request to the managed resource.

Profile version

Specifies the version of the profile that is installed in the Identity server.

TDI version

Specifies the version of the Security Directory Integrator on which the adapter is deployed.

Dispatcher version

Specifies the version of the Dispatcher.

Installation platform

Specifies summary information about the operating system where the adapter is installed.

Adapter account

Specifies the account that running the adapter binary file.

Adapter up time: Date

Specifies the date when the adapter started.

Adapter up time: Time

Specifies the time of the date when the adapter started.

Adapter memory usage

Specifies the memory usage for running the adapter.

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

- Verify the adapter log to ensure that the test request was sent successfully to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. Verify parameters such as the work station name or the IP address of the managed resource and the port.

Installing the ILMT tags

This topic describes the procedures to install ILMT tag files.

About this task

Ensure that the Dispatcher is installed.

Procedure

- Copy the files from **ILMT-Tags** folder to the specified location:
 - Windows: <SDI-HOME>/swidtag
 - Unix/Linux: <SDI-HOME>/swidtag

Verifying that the adapter is working correctly

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

Procedure

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

Chapter 4. Configuring

After you install the adapter, configure it to function correctly. Configuration is based on your requirements or preference.

See the *IBM Security Dispatcher Installation and Configuration Guide* for more configuration options such as:

- JVM properties
- Dispatcher filtering
- Dispatcher properties
- Dispatcher port number
- Logging configurations
- Secure Sockets Layer (SSL) communication

Customized attributes

Use these tasks to configure the Google Workspace Adapter to support customized Google Workspace attributes.

Google Workspace supports custom fields for the user object. However, the Google Workspace Adapter supports only the standard set of attributes.

You can customize the adapter to support custom attributes. Complete the following tasks to customize the Google Workspace Adapter to support custom fields in Google Workspace.

Schema extensions and custom attributes

Use the interface and tools that are provided by Google Workspace Adapter to extend the Google Workspace attributes.

For more information about adding new attributes to the Google Workspace User schema, see the Google Workspace documentation at <https://support.google.com/a/answer/6208725?hl=en>.

The current version of Google Workspace Adapter supports only the String type of custom attributes.

Note:

- Custom `Category` name must be `misc`.
- The custom attributes are supported for only `User` account class.
- Multiple `values` or `Private` settings are not supported.

Copying the `GoogleAppsProfile.jar` file and extracting files

Use these tasks to customize your environment.

About this task

The profile JAR file, `GoogleAppsProfile.jar`, is included in the Google Workspace Adapter compressed file that you downloaded from the IBM website. The `GoogleAppsProfile.jar` file contains a folder that is named **GoogleAppsProfile** with the following files:

- `CustomLabels.properties`
- `ergoogappsaccount.xml`
- `ergoogappsgroups.xml`
- `ergoogappsservice.xml`

- googleAppsAdd.xml
- GoogleAppsAssemblyLines.xml
- googleAppsDelete.xml
- googleAppsGroupAdd.xml
- googleAppsGroupDelete.xml
- googleAppsGroupModify.xml
- googleAppsModify.xml
- googleAppsSearch.xml
- googleAppsTest.xml
- schema.dsm1
- service.def
- targetProfile.json

You can modify these files to customize your environment. When you finish updating the profile JAR file, rebuild the JAR file and install it on the Identity server. For more information about the profile installation, see *Importing the adapter profile*.

Procedure

1. Log in to the system where the Google Workspace Adapter is installed.
2. On the **Start** menu, click **Programs > Accessories > Command Prompt**.
3. Copy the GoogleAppsProfile.jar file into a temporary directory.
4. Extract the contents of the GoogleAppsProfile.jar file into the temporary directory.

Run the following commands:

```
cd c:\temp
jar -xvf GoogleAppsProfile.jar
```

The **jar** command creates the c:\temp\GoogleAppsProfile directory.

What to do next

Edit the appropriate files by completing the following tasks.

Modifying the assembly lines

Use this task to add new mappings to the assembly lines for custom attributes.

About this task

The Google Workspace Adapter uses Security Directory Integrator to process requests before you submit them to Google Workspace.

The Google Workspace assembly lines contain mapping instructions from the IBM Security Verify Governance request to Google Workspace. Modify the assembly lines to add new mappings for custom attributes.

Procedure

1. Start the Security Directory Integrator Configuration Editor.
2. Open the googleAppsAdd.xml file. Complete these steps.
 - a) Click **File > Open Security Directory Integrator Configuration File...**
 - b) Browse to the GoogleAppsProfile directory.
 - c) Select the googleAppsAdd.xml file.

3. Optional: If previously edited, assign this configuration file to an existing project. Otherwise, proceed to the next screen to create a project and name it `googleAppsAdd`.
4. After the file is imported, expand the project to display the **AssemblyLines** tree in the Navigator pane.
5. Right click **googleAppsAdd assemblyline** and select **Open**. The **Add assemblyline** configuration is displayed in the main panel.
6. Click **Show Mapping** in the main panel. The mapping table for the assembly line is displayed in the main panel.
7. Under the **Data Flow** directory, click **Add**.
8. In the right pane, click **Add** to define a new attribute.
9. Under the **Add Attribute** window, enter the custom field name in the **Enter new name** box.

Note:

Use the name exactly as displayed in the API Name on the Google Workspace. For example, `CustomAttr`.

If a custom field name includes whitespace, then use underscore (`_`) to replace the whitespace. For example, if the Google Workspace custom field is `mail drop`, then enter `mail_drop` as a custom field.

10. Click **OK**.
11. Locate the newly added field in the mapping table and double-click the corresponding row to display an edit dialog box.
12. Change the default value of the custom field `work.[custom_field_name]` to `work.[custom_attribute_name]`.
For example, change the custom field `work.mail_drop` to `work.ergoogappsmaildrop`.
Prefix the attribute names with `ergoogapps` to easily identify the attributes that are used with IBM Security Verify Governance.
13. Move to **Schema** section in the right-most pane, right click, and select **Add**.
14. Under the **Input Schema Item** window, in the **Enter name for new Schema Item** box, enter the new `[custom_field_name]`.
For example, `mail_drop`.
15. Select the **Native Syntax** column for the new schema item and enter `java.lang.String`.
16. Click **File > Save**.
17. Right click the project in the Navigator pane and select the **Export...** option to export the new assembly line.
18. In the first screen of the **Export** dialog, expand the IBM Security Directory Integrator folder and select **Runtime Configuration**.
19. Click **Next**.
20. In the file path field, browse to the `GoogleAppsProfile` directory and select the file with the same name from step 2 to overwrite it.
21. Click **Finish**.
22. Repeat the steps 5 through 21 for the `GoogleAppsModify` assembly line.
23. Repeat steps 5 through 21 for the `GoogleAppsSearch` assembly line and do the following steps instead of steps 10 and 11:
 - a) Locate the field in the mapping table and click the **Work Attribute** cell corresponding to the custom field to rename it.
 - b) Enter the attribute name that is specified previously in step 11.
For example, `ergoogappsmaildrop`.

Updating the schema.dsm1 file

The Google Workspace Adapter schema.dsm1 file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Procedure

1. Locate the schema.dsm1 file in the \GoogleAppsProfile directory.
2. Edit the schema.dsm1 file to add an attribute definition for each custom attribute.

The Object Identifier (OID) is increased by 1, based on the last entry in the file.

For example, if the last attribute in the file uses the OID 1.3.6.1.4.1.6054.3.159.2.35, the first new attribute uses the OID 1.3.6.1.4.1.6054.3.159.2.36.

You might want to start a new range of numbers for your custom attributes. For example, start custom attributes with OID 1.3.6.1.4.1.6054.3.159.2.1000. This range prevents duplicate OIDs if the adapter is upgraded to support new attributes that are standard for newer versions of Google Workspace API.

3. Add each of the new attributes to the account class.
For example, add the following attribute definition under the erGoogleAppsAccount section of the schema.dsm1 file:

```
<attribute ref="ergoogappscustomattr" required="false"/>
```

4. Save the file.

Modifying the CustomLabels.properties file

After you add the custom attributes to the schema.dsm1 file, the attributes are available for use on the Google Workspace Adapter form.

About this task

The attributes are displayed in the attribute list for the account form. You can modify the attribute names that are in the attribute list.

To add the attribute and its corresponding label to the CustomLabels.properties file, complete the following steps:

Procedure

1. Locate the CustomLabels.properties file in the \GoogleAppsProfile directory.
2. Edit the CustomLabels.properties file to add the attribute and its corresponding label.

Use the following format:

```
attribute=label
```

Note: The attribute name must be in lowercase. For example:

```
##  
Adapter Labels definitions  
##  
ergoogappscustomattr=Custom Field One  
ergoogappscustomattrfield=Custom Attribute Field Two
```

3. Save the file.

Adapter form modification (optional)

After the changes are available in the Identity server, you can modify the Google Workspace Adapter forms to use the new custom attributes.

You do not have to add the attributes to the Google Workspace Adapter form unless you want them to be available. The attributes are returned during reconciliations unless you explicitly exclude them.

For more information about modifying the adapter form, see the IBM Security Verify Governance product documentation.

Editing Google Workspace Adapter profiles on the UNIX or Linux operating system

The adapter profile .jar file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character ^M at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the ^M characters. You can also use text editors, such as the **vi** editor, to remove the characters manually.

Example

You can use the **vi** editor to remove the ^M characters. From the **vi** command mode, run the following command and press Enter:

```
:%s/^M//g
```

When you use this command, enter ^M or **Ctrl -M** by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as a command.

Creating a JAR file and importing the profile

After you modify the schema .dsm1 or any other profile files, you must import these files, into IBM Security Verify Governance for the changes to take effect.

About this task

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the Identity server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see [Chapter 5, “Upgrading,” on page 27](#).

Procedure

1. Create a JAR file by using the files in the \temp directory. Run the following commands.

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

2. Import the GoogleAppsProfile.jar file into the Identity server. For more information about importing the file, see [#unique_38](#).
3. Stop and start the IBM Security Identity server.

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the Identity server to refresh the cache and the adapter schema

4. Import the GoogleAppsProfile.jar file into the Identity server.

5. Stop and start the Identity server.

Create a GoogleAppsCustomAttr.txt file with custom attributes

After you import the profile, you must define a file `GoogleAppsCustomAttr.txt` in the `ITDI_HOME\timso1` directory with custom attributes.

About this task

Note: If you are not using any custom attributes, then, do not define the `GoogleAppsCustomAttr.txt` file and do not create an empty file with the name `GoogleAppsCustomAttr.txt`.

Procedure

1. Create a file `GoogleAppsCustomAttr.txt` in the `ITDI_HOME\timso1` directory.
2. Open the file and list the custom attributes with the exact name that are defined in the Google Workspace console.

Note: If a custom field name includes whitespace, then use underscore (`_`) to replace the whitespace. For example, if the Google Workspace custom field is `mail drop`, then enter `mail_drop` as a custom field.

3. Define one attribute per line.
4. Save the file.

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 IBM Security Verify Governance.
2. Run a full reconciliation from IBM Security Verify Governance.
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 5. Upgrading

Upgrading an IBM Security Directory Integrator-based adapter involves tasks such as upgrading the dispatcher, the connector, and the adapter profile. Depending on the adapter, some of these tasks might not be applicable. Other tasks might also be required to complete the upgrade.

To verify the required version of these adapter components, see the adapter release notes.

Upgrading the adapter binaries or connector

Before you upgrade the connector, verify the version of the connector.

- If the connector version is higher or same as the previous version, the installer installs the new connector.
- If the connector version is lower than the existing connector version, the installer does not install the connector. A message is displayed indicating that no upgrade is required.

Note: Stop the dispatcher service before the upgrading the connector and start it again after the upgrade is complete.

Upgrading the adapter profile

Read the adapter Release Notes[®] for any specific instructions before you import a new adapter profile.

Note: Restart the Dispatcher service after importing the profile. Restarting the Dispatcher clears the assembly lines cache and ensures that the dispatcher runs the assembly lines from the updated adapter profile.

Upgrading the Google Directory API Java Client Library

Read the adapter Release Notes for any specific instructions before you copy the new Google Directory API Java Client Library.

See [“Installing 3rd party client libraries”](#) on page 7.

Note: Restart the dispatcher service after you copy the new Google Directory API Java Client Library.

Chapter 6. Troubleshooting

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

Techniques for troubleshooting problems

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

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

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

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

What are the symptoms of the problem?

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

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

Where does the problem occur?

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

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

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

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

When does the problem occur?

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

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

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

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

Under which conditions does the problem occur?

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

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

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

Can the problem be reproduced?

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

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

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

Related concepts

[Error messages and problem solving](#)

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

Error messages and problem solving

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

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

Table 5. Runtime problems

| Problem | Corrective Action |
|--|--|
| <p>Reconciliation does not return all Google Workspace accounts. Reconciliation is successful but some accounts are missing.</p> | <p>For the adapter to reconcile many accounts successfully, you might need to increase the WebSphere JVM memory. To complete the following steps on the WebSphere host computer:</p> <p>Note: Do not increase the JVM memory to a value higher than the system memory.</p> <ol style="list-style-type: none"> 1. Log in to the administrative console. 2. Expand Servers in the left menu and select Application Servers. 3. A table displays the names of known application servers on your system. Click the link for your primary application server. 4. Select Process Definition from the Configuration tab. 5. Select the Java Virtual Machine property. 6. Enter a new value for the Maximum Heap Size. The default value is 256 MB. <p>If the allocated JVM memory is not large enough, an attempt to reconcile many accounts with the adapter results in log file errors. The reconciliation process fails.</p> <p>The adapter log files contain entries that state <code>ErmpduAddEntry failed</code>. The <code>WebSphere_install_dir/logs/itim.log</code> file contains java.lang.OutOfMemoryError exceptions.</p> |

Related concepts

Techniques for troubleshooting problems

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

Chapter 7. Uninstalling

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

Removing the adapter binaries or connector

Use this task to remove the connector file for the Google Workspace Adapter.

About this task

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

Procedure

1. Stop the Dispatcher service.
2. Delete the JAR files that are listed in the [Chapter 3, "Installing," on page 7](#) section.
3. Start the Dispatcher service.

Deleting the adapter profile

Remove the adapter service/target type from the Identity server. Before you delete the adapter profile, ensure that no objects exist on the Identity server that reference the adapter profile.

Objects on the Identity server that can reference the adapter profile:

- Adapter service instances
- Policies referencing an adapter instance or the profile
- Accounts

Note: The Dispatcher component must be installed on your system for adapters to function correctly in a Security Directory Integrator environment. When you delete the adapter profile, do not uninstall the Dispatcher.

For specific information about how to delete the adapter profile, see the IBM Security Verify Governance product documentation.

Chapter 8. Reference

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

Adapter attributes and object classes

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

User attributes

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

| IBM Security Verify Governance name | Attribute name in schema | Data type |
|--|---------------------------------|------------------|
| User ID | eruid | String |
| Password | erpassword | Password |
| Given Name | ergoogappsgivenname | String |
| Family Name | ergoogappsfamilyname | String |
| Change Password on Next Login | ergoogappschgpwdnextlogin | String |
| Admin Privilege | ergoogappsadminprivilege | String |
| Group Membership multi-value attributes | ergoogappsgroupid | String |
| Alias | ergoogappsaliases | String |
| Organization Unit | ergoogappsoupath | String |
| Home Phone | ergoogappshomephone | String |
| Work Phone | ergoogappsworkphone | String |
| Mobile Phone | ergoogappsmobilephone | String |
| Home Address | ergoogappshomeaddress | String |
| Work Address | ergoogappsworkaddress | String |
| Manager's Email | ergoogappsmanageremail | String |
| Employee ID | ergoogappsemployeeid | String |
| Employee Title | ergoogappsemployeetitle | String |
| Employee Type | ergoogappsemployeetype | String |
| Organization | ergoogappsorganization | String |
| Department | ergoogappsdepartment | String |
| Cost Center | ergoogappscostcenter | String |

Group attributes

| IBM Security Verify Governance name | Attribute name in schema | Data type |
|-------------------------------------|--------------------------|-----------|
| Group Id | ergoogappsgroupid | String |
| Group Name | ergoogappsgroupname | String |
| Group Description | ergoogappsgroupdesc | String |
| Group Email Permission | ergoogappsemailperm | String |

Note:

- The **User Id** attribute is the Google Workspace User email address.
- The **Group Id** attribute is the Google Workspace Group email address. This attribute is mapped to the IBM Security Verify Governance **erGroupId**. You cannot use the adapter to modify this attribute.
- The **Group Name** attribute is mapped to the IBM Security Verify Governance **erGroupName** attribute. You cannot use the adapter to modify this attribute.
- The **Group Description** attribute cannot be modified to an empty string. This behavior is a known limitation of the Google Workspace Group Provisioning API. The adapter does not accept an empty string or null value.

Object classes

| Description | Object class name in schema | Superior |
|---------------|-----------------------------|----------|
| Service class | ergoogappsservice | Top |
| Account class | ergoogappsaccount | Top |
| Group class | ergoogappsgroups | Top |

Adapter Configuration Properties

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

Index

A

- adapter
 - features [1](#)
 - installation
 - troubleshooting errors [29](#)
 - warnings [29](#)
 - worksheet [6](#)
 - profile
 - upgrading [27](#)
 - uninstall [33](#)
- adapter form
 - modifying [25](#)
- adapters
 - removing profiles [33](#)
- attributes
 - customizing [21](#)
 - modifying the adapter form [25](#)
- automation of administrative tasks [1](#)

C

- components [2](#)
- configuration [2](#)
- connectors
 - upgrading [27](#)
- custom attributes
 - modifying CustomLabels.properties [24](#)
 - updating schema.dsml file [24](#)
- customizing attributes [21](#)
- CustomLabels.properties
 - modifying [24](#)

D

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

F

- files
 - CustomLabels.properties [24](#)
 - GoogleAppsProfile.jar [21](#)
 - schema.dsml [24](#)

I

- installation
 - adapter [7](#)
 - planning roadmaps [3](#)
 - uninstall [33](#)
 - worksheet [6](#)

J

- JAR files
 - extracting files [21](#)

M

- MS-DOS ASCII characters [25](#)

P

- profile
 - editing on UNIX or Linux [25](#)

R

- removing
 - adapter profiles [33](#)
- roadmaps
 - planning [3](#)

S

- schema.dsml
 - updating [24](#)
- service
 - restart [11](#)
 - start [11](#)
 - stop [11](#)
- software
 - download [5](#)
 - website [5](#)
- supported configurations [2](#)

T

- task automation [1](#)
- troubleshooting
 - identifying problems [29](#)
 - runtime problems [30](#)
 - techniques for [29](#)
- troubleshooting and support
 - troubleshooting techniques [29](#)

U

- upgrade
 - connectors [27](#)
- upgrades
 - adapter profiles [27](#)

V

- verification
 - dispatcher installation [7](#)

verifying the installation [26](#)

vi command [25](#)

