

IBM Security Verify Governance Identity  
Manager

*DB2 on z/OS Adapter Installation and  
Configuration Guide*





---

# Contents

- Figures..... V**
- Tables..... vii**
- Chapter 1. Overview..... 1**
  - Features.....1
  - Architecture.....1
  - Supported configurations..... 2
- Chapter 2. Planning..... 5**
  - Roadmap..... 5
  - Prerequisites..... 6
  - Software download..... 8
  - Installation worksheet..... 9
- Chapter 3. Installing..... 11**
  - Installing the dispatcher.....11
  - Installing the adapter binaries or connector.....12
  - Restarting the adapter service..... 13
  - Importing the adapter profile..... 13
  - Importing attribute mapping file..... 15
  - Adding a connector..... 16
  - Enabling connectors..... 18
  - Reviewing and setting channel modes for each new connector..... 20
  - Attribute Mapping..... 22
  - Service/Target form details..... 23
  - Verifying that the adapter is working correctly..... 26
- Chapter 4. Upgrading..... 29**
  - Upgrading the dispatcher..... 29
  - Upgrading the adapter profile..... 29
- Chapter 5. Configuring..... 31**
  - Customizing the adapter profile..... 31
  - Editing adapter profiles on the UNIX or Linux operating system..... 32
- Chapter 6. Troubleshooting..... 33**
  - Techniques for troubleshooting problems..... 33
  - Error messages and problem solving..... 35
- Chapter 7. Uninstalling..... 37**
  - Deleting the adapter profile..... 37
- Chapter 8. Reference..... 39**
  - Adapter attributes.....39
    - Attribute descriptions..... 39
    - Adapter attributes by action..... 47

**Index..... 51**

---

# Figures

- 1. The architecture of the IBM DB2 on z/OS adapter..... 2
- 2. Example of a single server configuration..... 3
- 3. Example of multiple server configuration..... 3



---

# Tables

- 1. Prerequisites to install the adapter.....7
- 2. Required information to install the adapter.....9
- 3. Prerequisites for enabling a connector.....18
- 4. Ports.....24
- 5. Warning and error messages ..... 35
- 6. Attributes, descriptions, and corresponding data types..... 39
- 7. Add request attributes..... 48
- 8. Change request attributes..... 49
- 9. Delete request attributes..... 50
- 10. Suspend request attributes..... 50
- 11. Restore attributes..... 50
- 12. Ping attributes..... 50
- 13. Reconciliation attributes..... 50





---

# Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The IBM® DB2 on z/OS adapter enables communication between the Identity server and the IBM DB2 on z/OS.

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

---

## Features

The adapter automates several administrative and management tasks.

- Reconciling user accounts and other support data
- Adding user accounts
- Modifying user account attributes
- Suspending, restoring, and deleting user accounts

### Related concepts

#### Architecture

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

#### Supported configurations

The adapter supports both single and multiple server configurations. There are two ways to configure the IBM DB2 on z/OS adapter. In a single server configuration, the adapter is installed on only one server. In a multiple server configuration, the adapter is installed on several different servers.

---

## Architecture

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

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

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

[Figure 1 on page 2](#) describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

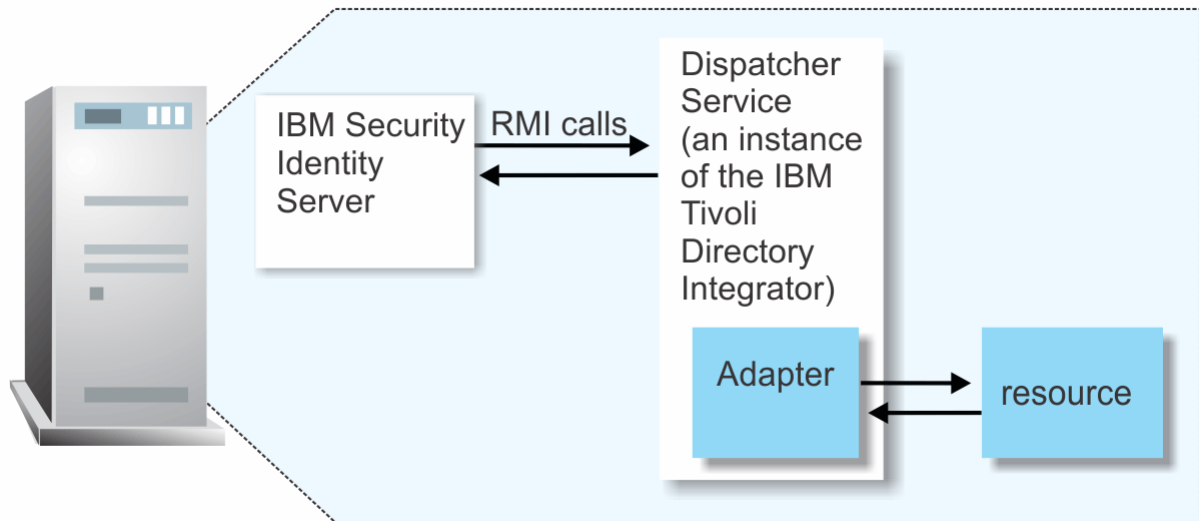


Figure 1. The architecture of the IBM DB2 on z/OS adapter

### Related concepts

#### Features

The adapter automates several administrative and management tasks.

#### Supported configurations

The adapter supports both single and multiple server configurations. There are two ways to configure the IBM DB2 on z/OS adapter. In a single server configuration, the adapter is installed on only one server. In a multiple server configuration, the adapter is installed on several different servers.

## Supported configurations

The adapter supports both single and multiple server configurations. There are two ways to configure the IBM DB2 on z/OS adapter. In a single server configuration, the adapter is installed on only one server. In a multiple server configuration, the adapter is installed on several different servers.

There are fundamental components in each environment:

- The Identity server
- The IBM Security Directory Integrator server
- The managed resource
- The adapter

The adapter must be installed directly on the server that runs the Security Directory Integrator server.

### Single server configuration

The Identity server, the Security Directory Integrator server, and the IBM DB2 on z/OS adapter are installed on one server to establish communication with the managed resource. The managed resource is installed on a different server as described [Figure 2 on page 3](#).

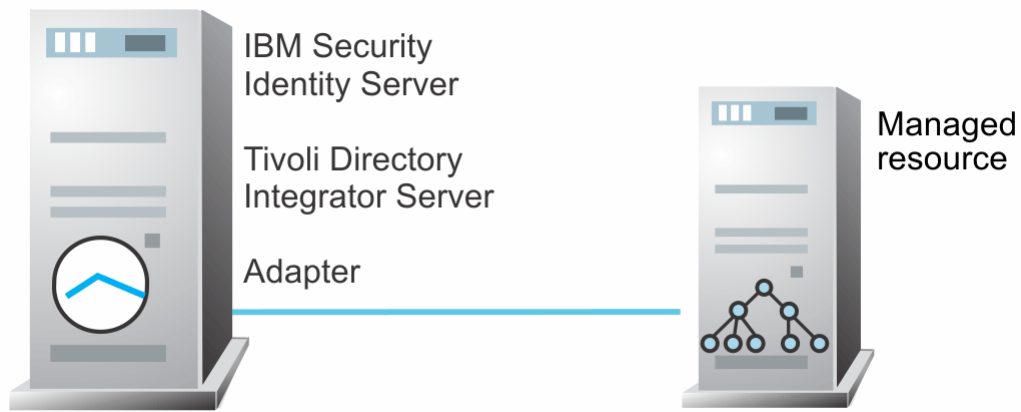


Figure 2. Example of a single server configuration

### Multiple server configuration

In multiple server configuration, the Identity server, the Security Directory Integrator server, and the IBM DB2 on z/OS are installed on different servers. The Security Directory Integrator server and the IBM DB2 on z/OS adapter are installed on the same server as described in [Figure 3 on page 3](#).



Figure 3. Example of multiple server configuration

### Related concepts

#### Features

The adapter automates several administrative and management tasks.

#### Architecture

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



---

## Chapter 2. Planning

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

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

---

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

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

#### Pre-installation

Complete these tasks.

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

#### Installation

Complete these tasks.

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

#### Upgrade

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

#### Configuration

Complete these tasks.

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

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

## Troubleshooting

See the following topics.

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

## Uninstallation

Complete these tasks.

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

## Reference

See the following topics.

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

### Related concepts

#### Prerequisites

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

#### Software download

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

#### 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.

## Prerequisites

---

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

[Table 1 on page 7](#) identifies the software and operating system prerequisites for the adapter installation.

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

Table 1. Prerequisites to install the adapter

| Prerequisite                   | Description   |
|--------------------------------|---|
| Directory Integrator           | <ul style="list-style-type: none"> <li>• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008</li> <li>• IBM Security Directory Integrator Version 7.2</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> </ul> |
| Identity server                | <p>The following servers are supported:</p> <ul style="list-style-type: none"> <li>• Identity server Version 10.0</li> <li>• Identity server Version 10.0</li> <li>• IBM Security Privileged Identity Manager Version 2.0</li> <li>• Identity server Version 10.0</li> </ul>  |
| IBM DB2 on z/OS                | <p>A z system that runs IBM DB2® with one of the following versions:</p> <ul style="list-style-type: none"> <li>• IBM DB2, Version 10 for z/OS®</li> <li>• IBM DB2, Version 11 for z/OS</li> </ul>  |
| IBM DB2 JDBC Driver            | <ul style="list-style-type: none"> <li>• db2jcc4.jar</li> <li>• db2jcc_license_cisuz.jar</li> </ul> <p>Copy the JDBC drivers , which are included with the adapter package, to the following location:</p> <p><b>Windows</b><br/> drive:\Program Files\IBM\TDI\TDI_VERSION\jars\3rdparty\IBM</p> <p><b>Unix</b><br/> /opt/IBM/TDI/TDI_VERSION/jars/3rdparty/IBM</p> <p><b>Note:</b> Delete the db2jcc.jar, if its present in the folder</p>   |
| Network Connectivity           | <p>Install the adapter on a workstation that can communicate with the IBM Security Verify Governance Identity Manager service through the TCP/IP network.</p>   |
| System Administrator Authority | <p>To complete the adapter installation procedure, you must have system administrator authority.</p>  |

| <i>Table 1. Prerequisites to install the adapter (continued)</i> |   |
|--|---|
| <b>Prerequisite</b>  | <b>Description</b>  |
| Security Directory Integrator adapters solution directory        | A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for adapters. See the <i>Dispatcher Installation and Configuration Guide</i> .  |
| IBM DB2 on z/OS Account, for example db2admin.                   | <p>You must provide a IBM DB2 on z/OS account and password for every IBM DB2 on z/OS instance that the adapter manages.</p> <p>The IBM DB2 on z/OS account must have the following IBM DB2 on z/OS privileges:</p> <p><b>SYSADM</b><br/>System administrator. An ID with SYSADM authority that grants the privileges to the group ID.</p> |

Install the IBM DB2 on z/OS adapter and the appropriate IBM DB2 JDBC drivers on the same workstation as the Security Directory Integrator.

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

### **Related concepts**

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

### Software download

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

### 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.

## **Software download**

---

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

Go to [IBM Passport Advantage](#).

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

### **Note:**

You can also obtain additional adapter information from IBM Support.

### **Related concepts**

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

### Prerequisites

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

### 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.

## 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> |  |   |
|---|--|---|
| <b>Required information</b>                                 | <b>Description</b>   | <b>Value</b>  |
| IBM Security Directory Integrator Home Directory            | The <i>ITDI_HOME</i> directory contains the <i>jars/connectors</i> subdirectory. This subdirectory contains adapter JAR files.   | <p>IBM Security Directory Integrator can be automatically installed with your IBM Security Verify Governance Identity Manager product.</p> <p>The following are the default directory path that is used for Security Directory Integrator:</p> <p><b>Windows:</b><br/> drive:\Program Files\IBM\TDI\TDI_VERSION</p> <p><b>UNIX:</b><br/> /opt/IBM/TDI/TDI_VERSION</p> |
| Adapters solution directory                                 | When you install the dispatcher, the adapter prompts you to specify a file path for the adapters solution directory. If you do not specify a directory, the default directory is <i>timsol</i> . | <p><b>Windows:</b><br/> drive:\Program Files\IBM\TDI\TDI_VERSION\timsol</p> <p><b>UNIX:</b><br/> /opt/IBM/TDI/TDI_VERSION/timsol</p>  |

### **Related concepts**

[Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Governance Identity Manager](#)

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

### [Prerequisites](#)

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

### [Software download](#)

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



---

## 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](#).

Depending on your adapter, the Security Directory Integrator connector might already be installed as part of the Security Directory Integrator product and no further action is required. If the connector is not pre-installed, install it after the Dispatcher.

---

### Installing the dispatcher

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

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

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

#### **Related concepts**

##### 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.

##### Service/Target form details

Complete the service/target form fields.

#### **Related tasks**

##### 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.

##### 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.

##### Importing attribute mapping file

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

##### Adding a connector

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

##### Enabling connectors

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

##### 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.

##### Attribute Mapping

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

[Verifying that the adapter is working correctly](#)

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

## 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.

### About this task

The adapter uses the IBM Security Directory Integrator JDBC connector. Follow the steps in the procedure to download and copy the JDBC Connector JAR. As such, you just need to install the Dispatcher. See the *IBM Security Dispatcher Installation and Configuration Guide*.

### Related concepts

[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.

[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.

[Service/Target form details](#)

Complete the service/target form fields.

### Related tasks

[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.

[Importing attribute mapping file](#)

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

[Adding a connector](#)

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

[Enabling connectors](#)

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

[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.

[Attribute Mapping](#)

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

[Verifying that the adapter is working correctly](#)

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

## 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*.

### Related concepts

#### 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.

#### Service/Target form details

Complete the service/target form fields.

### Related tasks

#### 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.

#### 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.

#### Importing attribute mapping file

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

#### Adding a connector

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

#### Enabling connectors

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

#### 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.

#### Attribute Mapping

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

#### Verifying that the adapter is working correctly

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

## Importing the adapter profile

---

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

### Before you begin

- The Identity server is installed and running.

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

## About this task

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

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

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

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

## Procedure

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage > Profiles**.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.
5. Click **Actions > Import**.
6. On the **Import** page, complete these steps:
  - a) Select **Profile**.
  - b) Click **Browse** to locate the JAR file that you want to import.
  - c) Click **Upload file**.  
A message indicates that you successfully imported a profile.
7. Click **Close**.  
The new profile is displayed in the list of profiles.

## Results

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

## What to do next

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

- Import the attribute mapping file. See [“Importing attribute mapping file” on page 15](#).
- Create a connector that uses the target profile. See [“Adding a connector” on page 16](#).

## Related concepts

[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.

#### 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.

#### Service/Target form details

Complete the service/target form fields.

### **Related tasks**

#### 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.

#### Importing attribute mapping file

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

#### Adding a connector

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

#### Enabling connectors

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

#### 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.

#### Attribute Mapping

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

#### Verifying that the adapter is working correctly

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

## **Importing attribute mapping file**

---

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

### **About this task**

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

### **Procedure**

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

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

c) Click **Upload file**.

A message indicates that you successfully imported the file.

7. Click **Close**.

### **Related concepts**

#### 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.

#### 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.

#### Service/Target form details

Complete the service/target form fields.

### **Related tasks**

#### 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.

#### 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.

#### Adding a connector

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

#### Enabling connectors

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

#### 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.

#### Attribute Mapping

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

#### Verifying that the adapter is working correctly

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

## **Adding a connector**

---

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

### **Before you begin**

Complete Importing the adapter profile.

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



## About this task

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

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

## Procedure

To add a connector, complete these steps.

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

## Results

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

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

## What to do next

Enable the channel modes to synchronize the data between the target systems and Verify Governance Identity Manager. For more information, see [“Enabling connectors” on page 18](#).

### Related concepts

#### [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.

#### [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.

#### Service/Target form details

Complete the service/target form fields.

#### **Related tasks**

##### 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.

##### 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.

##### Importing attribute mapping file

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

##### Enabling connectors

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

##### 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.

##### Attribute Mapping

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

##### Verifying that the adapter is working correctly

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

## 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

| Prerequisite   | Find more information  |
|--|--|
| A connector must exist in Verify Governance Identity Manager.            | <a href="#">“Adding a connector” on page 16.</a>   |
| Ensure that you enabled the appropriate channel modes for the connector. | <a href="#">“Reviewing and setting channel modes for each new connector” on page 20.</a> |

### Procedure

To enable a connector, complete these steps:

1. Log in to the Verify Governance Identity Manager Administration Console.
2. From the Administration Console, select **Enterprise Connectors**.
3. Select **Manage > Connectors**.  
A list of connectors is displayed on the **Connectors** tab.
4. Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

5. Optional: To view all of the columns in the list of connectors, expand the **Connectors** pane.
6. Select the connector that you want to enable.
7. On the **Connector Details** tab, complete these steps:
  - a) Select the channel modes that you want to enable, and then click **Save**. Depending on the channels that you enable, the corresponding **Channel** tabs are displayed.

#### **Enable write-to channel**

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

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

#### **Enable read-from channel**

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

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

#### **Enable reconciliation**

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

## **Results**

The connector is enabled

## **What to do next**

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

### **Related concepts**

#### 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.

#### 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.

#### Service/Target form details

Complete the service/target form fields.

### **Related tasks**

#### 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.

#### 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.

#### Importing attribute mapping file

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

#### Adding a connector

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

#### 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.

#### Attribute Mapping

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

#### Verifying that the adapter is working correctly

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

## **Reviewing and setting channel modes for each new connector**

---

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

### **About this task**

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

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

### **Procedure**

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

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

#### **Enable write-to channel**

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

#### **Enable read-from channel**

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

#### **Enable reconciliation**

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

8. Select **Monitor > Change Log Sync Status**.  
A list of connectors is displayed.
9. On the **Change Log Sync Status** tab, complete these steps:
  - a) Optional: Click **Filter** to toggle the filter on to refine your search results, or click **Hide Filter** to toggle the filter off. When the filter is visible, you can specify search criteria for your requests, and then click **Search**.

- b) Select a connector, and click **Actions > Sync Now**.  
The synchronization process begins.
  - c) Optional: To view the status of the synchronization request, select **Sync History** in the right pane.  
Information about the synchronization is displayed in the **Sync History** tab.
10. Set the change log synchronization schedule for each new connector that you migrated.
  11. When the connector configuration is complete, enable the connector by completing these steps:
    - a) Select **Manage > Connectors**.
    - b) Select the connector that you want to enable, and then select the **Enable** check box in the **Connector Details** tab.
    - c) Click **Save**.  
For more information, see [“Enabling connectors” on page 18](#).  
  
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**.

### **Related concepts**

#### 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.

#### 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.

#### Service/Target form details

Complete the service/target form fields.

### **Related tasks**

#### 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.

#### 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.

#### Importing attribute mapping file

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

#### Adding a connector

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

#### Enabling connectors

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

#### Attribute Mapping

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

#### Verifying that the adapter is working correctly

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

## Attribute Mapping

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

### About this task

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

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

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

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

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

#### Note:

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

### Procedure

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

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

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

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

5. Import the updated mapping definition file through the Enterprise Connectors module. For more information, see *Attribute-to-permission mapping service* in the IBM Security Verify Governance Identity Manager product documentation.
6. Map the following attributes for **Chanel-Write To** and **Chanel-Read From**

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

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

## Related concepts

### 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.

### 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.

### Service/Target form details

Complete the service/target form fields.

## Related tasks

### 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.

### 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.

### Importing attribute mapping file

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

### Adding a connector

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

### Enabling connectors

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

### 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.

### Verifying that the adapter is working correctly

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

## Service/Target form details

---

Complete the service/target form fields.

### **On the IBM DB2 on z/OS Connection tab:**

#### **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**

Optional: Specify a description that identifies the service for your environment.

#### **Tivoli® 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.

| <i>Table 4. Ports</i> |  |
|-----------------------|--|
| <b>Instance</b>       | <b>Ports</b>                             |
| 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

**IBM DB2 on z/OS Server Host**

Specify the host workstation on which the IBM DB2 on z/OS server is running.

**IBM DB2 on z/OS Server Port**

Specify the TCP port on which the IBM DB2 on z/OS server is running. You can specify 50000 to use the default DB2 port.

**IBM DB2 on z/OS Database Name**

Specify the database name of the IBM DB2 on z/OS database that you want to manage, for example SAMPLE.

**IBM DB2 on z/OS Administration User Account**

Specify the name of the user who has access to the IBM DB2 on z/OS resource and who can do administrative operations.

**IBM DB2 on z/OS Administration User Password**

Specify the password for the user.

**Owner**

Optionally, specify a user as a service owner.

**Service Prerequisite**

Specify a service that is prerequisite to this service.

**On the Dispatcher Attributes tab:**

**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.

**AL File System 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 the following file path to load the assembly lines from the profiles directory of the Windows operating system: `c:\Files\IBM\TDI\V7.1\profiles`.

Alternatively, you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating system: `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 if 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.

**On the Status and information tab**

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 is 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 successfully sent 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.

**Related concepts**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.

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.

**Related tasks**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.

#### 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.

#### Importing attribute mapping file

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

#### Adding a connector

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

#### Enabling connectors

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

#### 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.

#### Attribute Mapping

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

#### Verifying that the adapter is working correctly

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

## **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.

### **Related concepts**

#### 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.

#### 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.

#### Service/Target form details

Complete the service/target form fields.

### **Related tasks**

#### 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.

#### 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.

#### Importing attribute mapping file

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

#### Adding a connector

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

#### Enabling connectors

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

#### 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.

#### Attribute Mapping

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



---

## Chapter 4. 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.

### Upgrading the dispatcher

---

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

- If the dispatcher version mentioned in the release notes is later than the existing version on your workstation, install the dispatcher.
- If the dispatcher version mentioned in the release notes is the same or earlier than the existing version, do not install the dispatcher.

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

#### **Related concepts**

[Upgrading the adapter profile](#)

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

### 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.

#### **Related concepts**

[Upgrading the dispatcher](#)

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



---

## Chapter 5. 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

---

### Customizing the adapter profile

To customize the adapter profile, you must modify the IBM DB2 on z/OS adapter JAR file. You might customize the adapter profile to change the account form or the service form.

#### About this task

You can also use the Form Designer or the `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file for that adapter.

The JAR file is included in the IBM DB2 on z/OS adapter compressed file that you downloaded from the IBM website. The IBM DB2 on z/OS JAR file and the files that are contained in the JAR file vary depending on your operating system.

**Note:** You cannot modify the schema for this adapter. You cannot add or delete attributes from the schema.

The adapter JAR file includes the following files:

- `CustomLabels.properties`
- `erZDB2Account.xml`
- `erZDB2Service.xml`
- `schema.dsm1`
- `service.def`
- `ZDB2AddUserAL.xml`
- `ZDB2DeleteUserAL.xml`
- `ZDB2ModifyUserAL.xml`
- `ZDB2SearchUserAL.xml`
- `ZDB2TestAL.xml`

#### Procedure

- To edit the JAR file, take these steps:
  - a) Log on to the workstation where the IBM DB2 on z/OS adapter is installed.
  - b) On the **Start** menu, click **Programs → Accessories → Command Prompt**.
  - c) Copy the JAR file into a temporary directory.
  - d) Extract the contents of the JAR file into the temporary directory by running the following command.

The following example applies to the IBM DB2 on z/OS adapter profile. Type the name of the JAR file for your operating system.

```
cd c:\temp
jar -xvf ZDB2AdapterProfile.jar
```

The **jar** command extracts the files into the directory.

e) Edit the file that you want to change

After you edit the file, you must import the file into the Identity server for the changes to take effect.

- To import the file, take these steps:

a) Create a JAR file by using the files in the \temp directory.

Run the following commands:

```
cd c:\temp
jar -cvf ZDB2AdapterProfile.jar ZDB2AdapterProfile
```

b) Import the JAR file into the IBM Security Verify Governance Identity Manager application server.

c) Stop and start the Identity server

d) Restart the adapter service.

### Related tasks

[Editing 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.

## Editing 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.

### Related tasks

[Customizing the adapter profile](#)

To customize the adapter profile, you must modify the IBM DB2 on z/OS adapter JAR file. You might customize the adapter profile to change the account form or the service form.



---

# 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](#)

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

## Error messages and problem solving

A warning or error message might be displayed in the user interface to provide information about the adapter or when an error occurs.

A warning or error might be displayed in the user interface to provide information that you must know about the adapter or about an error. Table 5 on page 35 contains warnings or errors that might be displayed in the user interface if the IBM DB2 on z/OS adapter is installed on your system.

| Message code | Warning or error message  | Remedial action  |
|--------------|---|--|
| CTGIMT001E   | The following error occurred. Error: Either the IBM DB2 on z/OS service name is incorrect or the service is not up. | Ensure that the IBM DB2 on z/OS service name given on IBM Security Verify Governance Identity Manager service form is running.   |
| CTGIMT001E   | The following error occurred. Error: Either the IBM DB2 on z/OS host or port is incorrect.                          | Verify that the host workstation name or the port for the IBM DB2 on z/OS service is correctly specified.  |
| CTGIMT002E   | The login credential is missing or incorrect.   | Verify that you provided correct login credential on service form.   |
| CTGIMT001E   | The following error occurred. Error: No suitable JDBC driver found.   | Ensure that the correct version of the JDBC driver is copied onto the workstation where the adapter is installed. Ensure that the path for the driver is included in the system CLASSPATH variable.  |
| CTGIMT600E   | An error occurred while establishing communication with the IBM Security Directory Integrator server.               | IBM Security Verify Governance Identity Manager cannot establish a connection with IBM Security Directory Integrator. To fix this problem, ensure that: <ul style="list-style-type: none"> <li>• IBM Security Directory Integrator is running.</li> <li>• The URL specified on the service form for the IBM Security Directory Integrator is correct.</li> </ul> |
| CTGIMT003E   | The account already exists.   | Use a different name for the user to be added.   |
| CTGIMT015E   | An error occurred while deleting the <i>Account_Name</i> account because the account does not exist.                | The user you trying to delete does not exist. Ensure that you are deleting only an existing account.   |

### 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.

### Deleting the adapter profile

---

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

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

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

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

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



## Chapter 8. Reference

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

### Adapter attributes

As part of the adapter implementation, a dedicated account that allows IBM Security Verify Governance Identity Manager to access the IBM DB2 on z/OS is created on the IBM DB2 on z/OS.

The adapter consists of files and directories that are owned by the IBM Security Verify Governance Identity Manager account. These files establish communication with the Identity server.

### Attribute descriptions

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

The combination of attributes depends on the type of action that the IBM Security Verify Identity server requests from the adapter.

Table 6 on page 39 lists the account form attributes that the adapter uses.

| Attribute                           | Directory server attribute | Description   | Data format |
|-------------------------------------|----------------------------|---|-------------|
| Administration User Account         | erRmiZDBAdminName          | Specify the user ID that is used to connect to the IBM DB2 on z/OS. The value of this key must be the administrator user of the Cataloged database.<br>Administration User Account is the required field.                                   | String      |
| Administration User Password        | erServicePwd1              | Specify the password for the user ID that is used to connect to the IBM DB2 on z/OS. The value of this key must be the password of the administrator user of the Cataloged database.<br>Administration User Password is the required field. | String      |
| System privileges                   | erRmiZOSSysPriv            | Specifies the list of system privileges.  | String      |
| System privileges with grant option | erRmiZOSSysPrivGrant       | Specifies the list of system privileges with grant option   | String      |

Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute                     | Directory server attribute    | Description  | Data format |
|-------------------------------|-------------------------------|--|-------------|
| PrivCreateinSchema            | erRmiZDBPrivCreateinSchema    | Specifies all schemas on which the privilege to create objects in the schema is granted to the user.<br>It is multivalued.                 | String      |
| erRmiZDBPrivWGrCreateinSchema | erRmiZDBPrivWGrCreateinSchema | Specifies all schemas on which the privilege to create objects in the schema is granted to the user.<br>It is multivalued.                 | String      |
| PrivAlterinSchema             | erRmiZDBPrivAlterinSchema     | Specifies all schemas on which the privilege to alter objects in the schema is granted to the user.<br>It is multivalued.                  | String      |
| PrivWGrAlterinSchema          | erRmiZDBPrivWGrAlterinSchema  | Specifies all schemas on which the privilege to alter objects in the schema with grant option is granted to the user.<br>It is multivalued | String      |
| ZDBPrivDropinSchema           | erRmiZDBPrivDropinSchema      | Specifies all schemas on which the privilege to drop objects in the schema is granted to the user.<br>It is multivalued.                   | String      |
| ZDBPrivWGrDropinSchema        | erRmiZDBPrivWGrDropinSchema   | Specifies all schemas on which the privilege to drop objects in the schema with grant option is granted to the user.<br>It is multivalued. | String      |
| PrivSelectTab                 | erRmiZDBPrivSelectTab         | Specifies all tables on which the select privilege is granted to the user.<br>It is multivalued.   | String      |
| PrivWGrSelectTab              | erRmiZDBPrivWGrSelectTab      | Specifies all tables on which the select privilege with grant option is granted to the user.<br>It is multivalued.                         | String      |



Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute        | Directory server attribute | Description  | Data format |
|------------------|----------------------------|--|-------------|
| PrivInsertTab    | erRmiZDBPrivInsertTab      | Specifies all tables on which the insert privilege is granted to the user. It is multivalued.                      | String      |
| PrivWFRInsertTab | erRmiZDBPrivWGrInsertTab   | Specifies all tables on which the Insert privilege with grant option is granted to the user.<br>It is multivalued. | String      |
| PrivUpdateTab    | erRmiZDBPrivUpdateTab      | Specifies all tables on which the Update privilege is granted to the user.<br>It is multivalued.                   | String      |
| PrivWGrUpdateTab | erRmiZDBPrivWGrUpdateTab   | Specifies all tables on which the Update privilege with grant option is granted to the user.<br>It is multivalued. | String      |
| PrivDeleteTab    | erRmiZDBPrivDeleteTab      | Specifies all tables on which the Delete privilege is granted to the user.<br>It is multivalued.                   | String      |
| PrivWGrDeleteTab | erRmiZDBPrivWGrDeleteTab   | Specifies all tables on which the Delete privilege with grant option is granted to the user.<br>It is multivalued. | String      |
| PrivAlterTab     | erRmiZDBPrivAlterTab       | Specifies all tables on which the Alter privilege is granted to the user.<br>It is multivalued.                    | String      |
| PrivWGrAlterTab  | erRmiZDBPrivWGrAlterTab    | Specifies all tables on which the Alter privilege with grant option is granted to the user.<br>It is multivalued.  | String      |
| PrivIndexTab     | erRmiZDBPrivIndexTab       | Specifies all tables on which the Index privilege is granted to the user.<br>It is multivalued.                    | String      |

Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute          | Directory server attribute | Description  | Data format |
|--------------------|----------------------------|--|-------------|
| PrivWGrIndexTab    | erRmiZDBPrivWGrIndexTab    | Specifies all tables on which the Index privilege with grant option is granted to the user.<br>It is multivalued.      | String      |
| PrivRefTab         | erRmiZDBPrivRefTab         | Specifies all tables on which the References privilege is granted to the user.<br>It is multivalued.                   | String      |
| PrivWGrRefTab      | erRmiZDBPrivWGrRefTab      | Specifies all tables on which the References privilege with grant option is granted to the user.<br>It is multivalued. | String      |
| PrivUseTabSpace    | erRmiZDBPrivUseTabSpace    | Specifies all schemas on which the use privilege is granted to the user.<br>It is multivalued.                         | String      |
| PrivWGrUseTabSpace | erRmiZDBPrivWGrUseTabSpace | Specifies all schemas on which the use privilege with grant option is granted to the user.<br>It is multivalued.       | String      |
| PrivSelectView     | erRmiZDBPrivSelectView     | Specifies all views on which the select privilege is granted to the user. It is multivalued.                           | String      |
| PrivWGrSelectView  | erRmiZDBPrivWGrSelectView  | Specifies all views on which the select privilege with grant option is granted to the user.<br>It is multivalued.      | String      |
| PrivInsertView     | erRmiZDBPrivInsertView     | Specifies all views on which the Insert privilege is granted to the user.<br>It is multivalued.                        | String      |
| PrivWGrInsertView  | erRmiZDBPrivWGrInsertView  | Specifies all views on which the Insert privilege with grant option is granted to the user.<br>It is multivalued.      | String      |

Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute           | Directory server attribute  | Description   | Data format |
|---------------------|-----------------------------|---|-------------|
| PrivUpdateView      | erRmiZDBPrivUpdateView      | Specifies all views on which the Update privilege is granted to the user.<br>It is multivalued.                           | String      |
| PrivWGrUpdateView   | erRmiZDBPrivWGrUpdateView   | Specifies all views on which the Update privilege with grant option is granted to the user.<br>It is multivalued.         | String      |
| PrivVwDeleteView    | erRmiZDBPrivVwDeleteView    | Specifies all views on which the Delete privilege is granted to the user.<br>It is multivalued.                           | String      |
| PrivWgrVwDeleteView | erRmiZDBPrivWGrVwDeleteView | Specifies all views on which the Delete privilege with grant option is granted to the user.<br>It is multivalued.         | String      |
| DBCreateTab         | erRmiDBCreateTab            | Specifies all Databases on which the Create Tab privilege is granted to the user.<br>It is multivalued.                   | String      |
| DBWGrCreateTab      | erRmiDBWGrCreateTab         | Specifies all Databases on which the Create Tab privilege with grant option is granted to the user.<br>It is multivalued. | String      |
| DBCreateTs          | erRmiDBCreateTs             | Specifies all Databases on which the Creates privilege is granted to the user.<br>It is multivalued.                      | String      |
| DBWGrCreateTs       | erRmiDBWGrCreateTs          | Specifies all Databases on which the CreateTs privilege with grant option is granted to the user.<br>It is multivalued.   | String      |
| DBDrop              | erRmiDBDrop                 | Specifies all Databases on which the dropdb privilege is granted to the user.<br>It is multivalued.                       | String      |

Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute      | Directory server attribute | Description  | Data format |
|----------------|----------------------------|--|-------------|
| DBWgrDrop      | erRmiDBWgrDrop             | Specifies all Databases on which the dropdb privilege with grant option is granted to the user.<br>It is multivalued.    | String      |
| DBDisplayDb    | erRmiDBDisplayDb           | Specifies all Databases on which the displaydb privilege is granted to the user.<br>It is multivalued.                   | String      |
| DBWgrDisplayDb | erRmiDBWgrDisplayDb        | Specifies all Databases on which the displaydb privilege with grant option is granted to the user.<br>It is multivalued. | String      |
| DbImagCopy     | erRmidbImagCopy            | Specifies all Databases on which the imagcopy privilege is granted to the user.<br>It is multivalued.                    | String      |
| DbWgrImagCopy  | erRmidbWgrImagCopy         | Specifies all Databases on which the imagcopy privilege with grant option is granted to the user.<br>It is multivalued.  | String      |
| DBLoad         | erRmiDBLoad                | Specifies all Databases on which the load privilege is granted to the user.<br>It is multivalued.                        | String      |
| DBWgrLoad      | erRmiDBWgrLoad             | Specifies all Databases on which the load privilege with grant option is granted to the user.<br>It is multivalued.      | String      |
| DBRecoverDb    | erRmiDBRecoverDb           | Specifies all Databases on which the recover privilege is granted to the user.<br>It is multivalued.                     | String      |

Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute      | Directory server attribute | Description   | Data format |
|----------------|----------------------------|---|-------------|
| DBWgrRecoverDb | erRmiDBWgrRecoverDb        | Specifies all Databases on which the recover privilege with grant option is granted to the user. It is multivalued. | String      |
| DBReorg        | erRmiDBReorg               | Specifies all Databases on which the reorg privilege is granted to the user. It is multivalued.                     | String      |
| DBWgrReorg     | erRmiDBWgrReorg            | Specifies all Databases on which the reorg privilege with grant option is granted to the user. It is multivalued.   | String      |
| DBStartDb      | erRmiDBStartDb             | Specifies all Databases on which the startdb privilege is granted to the user. It is multivalued.                   | String      |
| DBWgrStartDb   | erRmiDBWgrStartDb          | Specifies all Databases on which the startdb privilege with grant option is granted to the user. It is multivalued. | String      |
| DBRepair       | erRmiDBRepair              | Specifies all Databases on which the repair privilege is granted to the user. It is multivalued.                    | String      |
| DBWgrRepair    | erRmiDBWgrRepair           | Specifies all Databases on which the repair privilege with grant option is granted to the user. It is multivalued.  | String      |
| DBStats        | erRmiDBStats               | Specifies all Databases on which the stats privilege is granted to the user. It is multivalued.                     | String      |

Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute   | Directory server attribute | Description  | Data format |
|-------------|----------------------------|--|-------------|
| DBWgrStats  | erRmiDBWgrStats            | Specifies all Databases on which the stats privilege with grant option is granted to the user. It is multivalued.  | String      |
| DBStopdb    | erRmiDBStopdb              | Specifies all Databases on which the stopdb privilege is granted to the user. It is multivalued.                   | String      |
| DBWgrStopdb | erRmiDBWgrStopdb           | Specifies all Databases on which the stopdb privilege with grant option is granted to the user. It is multivalued. | String      |
| DBDbadm     | erRmiDBDbadm               | Specifies all Databases on which the dbadm privilege is granted to the user. It is multivalued.                    | String      |
| DBWgrDbadm  | erRmiDBWgrDbadm            | Specifies all Databases on which the dbadm privilege with grant option is granted to the user. It is multivalued.  | String      |
| DBCtrl      | erRmiDBCtrl                | Specifies all Databases on which the dbctrl privilege is granted to the user. It is multivalued.                   | String      |
| DBWgrCtrl   | erRmiDBWgrCtrl             | Specifies all Databases on which the dbctrl privilege with grant option is granted to the user. It is multivalued. | String      |
| DBMaint     | erRmiDBMaint               | Specifies all Databases on which the dbmaint privilege is granted to the user. It is multivalued.                  | String      |

Table 6. Attributes, descriptions, and corresponding data types (continued)

| Attribute  | Directory server attribute | Description  | Data format |
|------------|----------------------------|--|-------------|
| DBWgrMaint | erRmiDBWgrMaint            | Specifies all Databases on which the dbmaint privilege with grant option is granted to the user.<br><br>It is multivalued. | String      |

**Related reference**

[Adapter attributes by action](#)

The following lists describe typical adapter actions that are organized by their functional transaction group. The lists include more information about required and optional attributes that are sent to the adapter to complete that action.

**Adapter attributes by action**

The following lists describe typical adapter actions that are organized by their functional transaction group. The lists include more information about required and optional attributes that are sent to the adapter to complete that action.

**Related reference**

[Attribute descriptions](#)

The Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

## Database login add

A database login add is a request to create a user account with the specified attributes.

| Table 7. Add request attributes |                               |                     |
|---------------------------------|-------------------------------|---------------------|
| Required attribute              | Optional attribute            |                     |
| eruid                           | erRmiZOSSysPrivGrant          | erRmiDBCreateTab    |
| erRmiZOSSysPriv                 | erRmiZDBPrivCreateinSchema    | erRmiDBWGrCreateTab |
|                                 | erRmiZDBPrivWGrCreateinSchema | erRmiDBCreateTs     |
|                                 | erRmiZDBPrivAlterinSchema     | erRmiDBWGrCreateTs  |
|                                 | erRmiZDBPrivWGrAlterinSchema  | erRmiDBDrop         |
|                                 | erRmiZDBPrivDropinSchema      | erRmiDBWGrDrop      |
|                                 | erRmiZDBPrivWGrDropinSchema   | erRmiDBDisplayDb    |
|                                 | erRmiZDBPrivSelectTab         | erRmiDBWGrDisplayDb |
|                                 | erRmiZDBPrivWGrSelectTab      | erRmiDbImagCopy     |
|                                 | erRmiZDBPrivInsertTab         | erRmiDbWGrImagCopy  |
|                                 | erRmiZDBPrivWGrInsertTab      | erRmiDBLoad         |
|                                 | erRmiZDBPrivUpdateTab         | erRmiDBWGrLoad      |
|                                 | erRmiZDBPrivWGrUpdateTab      | erRmiDBRecoverDb    |
|                                 | erRmiZDBPrivDeleteTab         | erRmiDBWGrRecoverDb |
|                                 | erRmiZDBPrivWGrDeleteTab      | erRmiDBReorg        |
|                                 | erRmiZDBPrivAlterTab          | erRmiDBWGrReorg     |
|                                 | erRmiZDBPrivWGrAlterTab       | erRmiDBStartDb      |
|                                 | erRmiZDBPrivIndexTab          | erRmiDBWGrStartDb   |
|                                 | erRmiZDBPrivWGrIndexTab       | erRmiDBRepair       |
|                                 | erRmiZDBPrivRefTab            | erRmiDBWGrRepair    |
|                                 | erRmiZDBPrivWGrRefTab         | erRmiDBStats        |
|                                 | erRmiZDBPrivUseTabSpace       | erRmiDBWGrStats     |
|                                 | erRmiZDBPrivWGrUseTabSpace    | erRmiDBStopdb       |
|                                 | erRmiZDBPrivSelectView        | erRmiDBWGrStopdb    |
|                                 | erRmiZDBPrivWGrSelectView     | erRmiDBDbadm        |
|                                 | erRmiZDBPrivInsertView        | erRmiDBWGrDbadm     |
|                                 | erRmiZDBPrivWGrInsertView     | erRmiDBCtrl         |
|                                 | erRmiZDBPrivUpdateView        | erRmiDBWGrCtrl      |
|                                 | erRmiZDBPrivWGrUpdateView     | erRmiDBMaint        |
|                                 | erRmiZDBPrivVwDeleteView      | erRmiDBWGrMaint     |
|                                 | erRmiZDBPrivWGrVwDeleteView   |                     |



## Database login change

A database login change is a request to change one or more attributes for the specified users.

| Required attribute | Optional attribute   |
|--------------------|--|
| eruid              | erRmiZOSSysPrivGrant<br>erRmiZOSSysPriv<br>erRmiZDBPrivCreateinSchema<br>erRmiZDBPrivWGrCreateinSchema<br>erRmiZDBPrivAlterinSchema<br>erRmiZDBPrivWGrAlterinSchema<br>erRmiZDBPrivDropinSchema<br>erRmiZDBPrivWGrDropinSchema<br>erRmiZDBPrivSelectTab<br>erRmiZDBPrivWGrSelectTab<br>erRmiZDBPrivInsertTab<br>erRmiZDBPrivWGrInsertTab<br>erRmiZDBPrivUpdateTab<br>erRmiZDBPrivWGrUpdateTab<br>erRmiZDBPrivDeleteTab<br>erRmiZDBPrivWGrDeleteTab<br>erRmiZDBPrivAlterTab<br>erRmiZDBPrivWGrAlterTab<br>erRmiZDBPrivIndexTab<br>erRmiZDBPrivWGrIndexTab<br>erRmiZDBPrivRefTab<br>erRmiZDBPrivWGrRefTab<br>erRmiZDBPrivUseTabSpace<br>erRmiZDBPrivWGrUseTabSpace<br>erRmiZDBPrivSelectView<br>erRmiZDBPrivWGrSelectView<br>erRmiZDBPrivInsertView<br>erRmiZDBPrivWGrInsertView<br>erRmiZDBPrivUpdateView<br>erRmiZDBPrivWGrUpdateView<br>erRmiZDBPrivVwDeleteView<br>erRmiZDBPrivWGrVwDeleteView |
|                    | erRmiDBCreateTab<br>erRmiDBWGrCreateTab<br>erRmiDBCreateTs<br>erRmiDBWGrCreateTs<br>erRmiDBDrop<br>erRmiDBWGrDrop<br>erRmiDBDisplayDb<br>erRmiDBWGrDisplayDb<br>erRmidbImagCopy<br>erRmidbWgrImagCopy<br>erRmiDBLoad<br>erRmiDBWgrLoad<br>erRmiDBRecoverDb<br>erRmiDBWgrRecoverDb<br>erRmiDBReorg<br>erRmiDBWgrReorg<br>erRmiDBStartDb<br>erRmiDBWgrStartDb<br>erRmiDBRepair<br>erRmiDBWgrRepair<br>erRmiDBStats<br>erRmiDBWgrStats<br>erRmiDBStopdb<br>erRmiDBWgrStopdb<br>erRmiDBDbadm<br>erRmiDBWgrDbadm<br>erRmiDBCtrl<br>erRmiDBWgrCtrl<br>erRmiDBMaint<br>erRmiDBWgrMaint  |

## Database login delete

A database login delete is a request to remove the specified user from the directory.

| <i>Table 9. Delete request attributes</i> |                    |
|---|--------------------|
| Required attribute                        | Optional attribute |
| erUid                                     | None               |

## Database login suspend

A database login suspend is a request to disable a user account.

The user is not removed. User attributes are not modified.

| <i>Table 10. Suspend request attributes</i> |                    |
|---|--------------------|
| Required attribute                          | Optional attribute |
| erUid<br>erAccountStatus                    | None               |

## Database login restore

A database login restore is a request to activate a user account that was previously suspended.

After an account is restored, the user can access the system by using the same attributes as the ones before the Suspend function was called.

| <i>Table 11. Restore attributes</i> |                    |
|-------------------------------------|--------------------|
| Required attribute                  | Optional attribute |
| erUid<br>erAccountStatus            | None               |

## Ping

Use Ping to verify connection between the adapter and the Identity server. Ping does not require any variables.

| <i>Table 12. Ping attributes</i> |                    |
|----------------------------------|--------------------|
| Required attribute               | Optional attribute |
| None                             | None               |

## Reconciliation

The reconciliation function synchronizes user account information between IBM Security Verify Governance Identity Manager and the adapter.

| <i>Table 13. Reconciliation attributes</i> |  |
|--|--|
| Attribute                                  |  |
| All supported attributes                   |  |

---

# Index

## A

adapter  
  customization steps [31](#)  
  features [1](#)  
  installation [11](#)  
  installation worksheet [9](#)  
  profile  
    upgrading [29](#)  
  supported configurations [2](#)  
  uninstall [37](#)  
  upgrading [29](#)  
adapter installation  
  troubleshooting errors [33](#)  
  warnings [33](#)  
adapter overview [1](#)  
adapters  
  removing profiles [37](#)  
add request attributes [48](#)  
attributes  
  adapter action, by  
    adding [48](#)  
    changing [49](#)  
    deleting [50](#)  
    modifying [49](#)  
    pinging [50](#)  
    restoring [50](#)  
    suspending [50](#)  
  description [39](#)  
  descriptions [39](#)  
  reconciliation [50](#)

## C

change request attributes [49](#)

## D

delete request attributes [50](#)  
dispatcher  
  installation [11](#)  
  upgrading [29](#)  
download, software [8](#)

## E

error messages [35](#)

## I

installation  
  adapter [11](#)  
  adapter software [12](#)  
  first steps [31](#)  
  planning roadmaps [5](#)  
  uninstall [37](#)

installation (*continued*)  
  worksheet [9](#)

## M

messages  
  error [35](#)  
  warning [35](#)  
MS-DOS ASCII characters [32](#)

## O

operating system prerequisites [6](#)  
overview [1](#)

## P

ping request attributes [50](#)  
profile  
  editing on UNIX or Linux [32](#)

## R

reconciliation attributes [50](#)  
removing  
  adapter profiles [37](#)  
request attributes  
  add [48](#)  
  change [49](#)  
  delete [50](#)  
  ping [50](#)  
  restore [50](#)  
  suspend [50](#)  
restore request attributes [50](#)  
roadmaps  
  planning [5](#)

## S

service  
  restart [13](#)  
  start [13](#)  
  stop [13](#)  
software  
  download [8](#)  
  website [8](#)  
software requirements [6](#)  
supported configurations  
  adapter [2](#)  
  overview [2](#)  
suspend request attributes [50](#)

## T

troubleshooting  
  error messages [35](#)

troubleshooting (*continued*)  
  identifying problems [33](#)  
  techniques for [33](#)  
  warning messages [35](#)  
troubleshooting and support  
  troubleshooting techniques [33](#)

## U

uninstallation [37](#)  
updating  
  adapter profile [31](#)  
upgrades  
  adapter [29](#)  
  adapter profiles [29](#)  
  dispatcher [29](#)

## V

verification  
  dispatcher installation [11](#)  
  operating system prerequisites [6](#)  
  operating system requirements [6](#)  
  software prerequisites [6](#)  
  software requirements [6](#)  
vi command [32](#)

## W

warning messages [35](#)



