IBM Security Identity Governance and Intelligence

CyberArk adapter Installation and Configuration Guide

IBM Security Identity Governance and Intelligence

CyberArk adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the IBM® Security Identity server. The CyberArk adapter enables communication between the IBM Security Identity server and the CyberArk SCIM server.

Features of the adapter

The CyberArk adapter automates several administrative and management tasks

You can perform the following tasks with the CyberArk adapter:

- Adding user accounts
- Changing user account passwords
- Modifying user account attributes
- Suspending and restoring user accounts
- Retrieving user accounts for the first time
- Deleting user accounts
- Reconciliation of modified user accounts
- Reconciliation of support data as Groups, Containers and Privileged Data

Architecture

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

The adapter requires the following components:

- Dispatcher
- Tivoli® Directory Integrator connector
- IBM Security Identity Adapter profile

Figure 1 describes the components that work together to complete the user account management tasks in a Tivoli Directory Integrator environment.

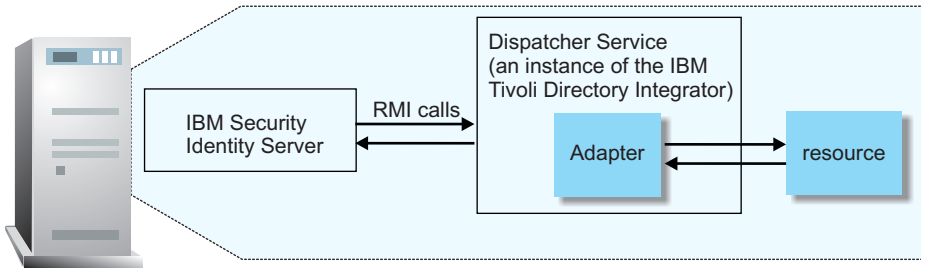

Figure 1. The architecture of the CyberArk adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

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

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

Single server configuration

In a single server configuration, the following components are installed on one server to establish communication with the CyberArk SCIM server:

- IBM Security Identity server
- Tivoli Directory Integrator server
- CyberArk adapter

The CyberArk SCIM server is installed on a different server as shown in Figure 2.

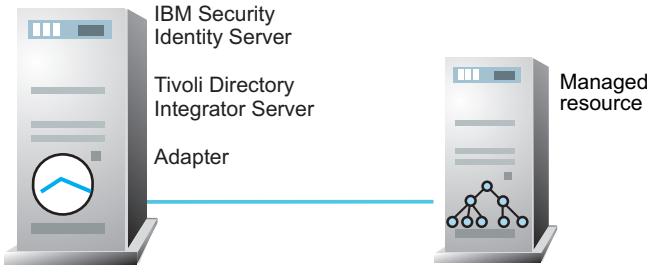

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the following components are installed on different servers.

- IBM Security Identity server
- Tivoli Directory Integrator server
- CyberArk adapter
- CyberArk SCIM server

TheTivoli Directory Integrator server and the CyberArk adapter are installed on the same server as shown in Figure 3 on page 3.

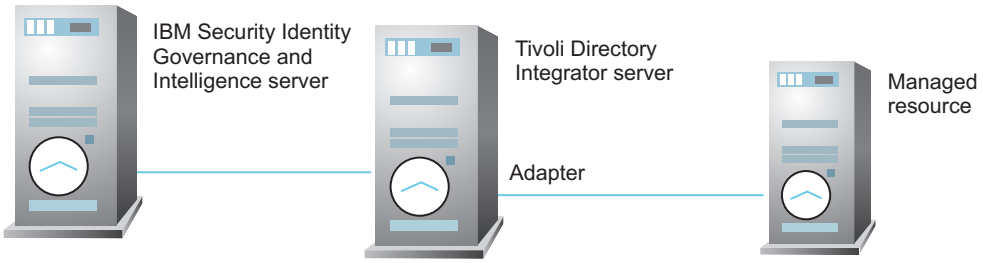

Figure 3. Example of a multiple server configuration

Chapter 2. Planning

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

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

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

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

Pre-installation

Complete these tasks.

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

Installation

Complete these tasks.

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

Upgrade

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

Configuration

Complete these tasks.

1. Configure secure communication between the IBM Security Identity server and the adapter.

a. Configure 1-way authentication.
b. Configure 2-way authentication.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Prerequisites

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

Table 1 identifies the prerequisites for the adapter installation.

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Directory Integrator	• IBM Tivoli Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Tivoli Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
IBM Security Identity server	The following servers are supported: • IBM Security Identity Governance and Intelligence Version 5.2.4.
CyberArk SCIM server	CyberArk v10.1.1
Tivoli Directory Integrator adapters solution directory	A Tivoli Directory Integrator work directory for adapters. For more information, see, the *Dispatcher Installation and Configuration Guide*.
System administrator authority	You must have system administrator authority to complete the adapter installation procedure.

Software downloads

Log in to your account on the IBM Passport Advantage® website and download the software.

Go to IBM Passport Advantage. See the *IBM Security Identity Governance and Intelligence Download Document*.

Note: You can also obtain adapter information from IBM Support.

Installation worksheet

The installation worksheet lists the information that is required to install and configure the adapter. Complete this worksheet before you start the installation procedure for ease of reference. Make a copy of the worksheet for each adapter instance you install.

Table 2. Required information to install the adapter

Required information	Description	Value
Tivoli Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory, which contains the files for the adapters.	**Windows:** *drive*`\Program Files\IBM\TDI\V7.2` **UNIX:** `/opt/IBM/TDI/V7.2`
Adapter Solution Directory	See the *Dispatcher Installation and Configuration Guide*.	**Windows:** *drive*`\Program Files\IBM\TDI\V7.2\`*timsol* **UNIX:** `/opt/IBM/TDI/V7.2/`*timsol*
Administrator account ID and password	An administrator account ID and password on the managed resource that has administrative rights for running the CyberArk adapter.	

Chapter 3. Installing

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

All IBM Tivoli Directory Integrator based adapters require the Dispatcher for the adapters to function correctly. If the Dispatcher is installed from a previous installation, do not reinstall it unless the Dispatcher is upgraded. See "Installing the dispatcher."

Depending on your adapter, the Tivoli Directory Integrator connector might already be installed as part of the Tivoli 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 Tivoli Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Tivoli Directory Integrator server where you want to install the adapter.

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

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

Installing third-party client libraries

The adapter requires access to the jars at runtime.

Copy the following list of JAR files to `ITDI_HOME/jars/3rdparty/others` folder:

- `httpclient-4.5.5.jar`
- `httpcore-4.4.9.jar`
- `jackson-annotations-2.5.0.jar`
- `jackson-core-2.5.0.jar`
- `jackson-databind-2.5.0.jar`

Installing the adapter binaries or connector

The adapter binaries establish that communication to the managed target. Some adapters relies on the Security Directory Integrator and don't include any binaries. For those adapters that do provide binary distribution, follow the adapter's installation steps.

Before you begin

- The Dispatcher must be installed.

Procedure

Copy CyberArkConnector.jar from the adapter package to the *ITDI_HOME*/jars/connectors directory.

Verifying the adapter installation

After you install the adapter, verify the adapter components on the IBM Tivoli Directory Integrator server. If the adapter is installed correctly, the adapter JAR file exists in the specified directory. If the JAR file does not exist, the installation is not successful and the adapter cannot function as expected. You must copy the JAR file in the specified location.

These adapter components must exist on the IBM Tivoli Directory Integrator server.

Table 3. Adapter components

Directory	Adapter component
ITDI_HOME/jars/connectors	CyberArkConnector.jar
ITDI_HOME/jars/3rdparty/other	• httpclient-4.5.5.jar • httpcore-4.4.9.jar • jackson-annotations-2.5.0.jar • jackson-core-2.5.0.jar • jackson-databind-2.5.0.jar

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. For example, you must restart the adapter if there are changes in the adapter profile, connector, or assembly lines. To restart the adapter, restart the Dispatcher.

The adapter does not exist as an independent service or a process. The adapter is added to the Dispatcher instance, which runs all the adapters that are installed on the same Security Directory Integrator instance.

See the topic about starting, stopping, and restarting the Dispatcher service in the *Dispatcher Installation and Configuration Guide*.

Importing the adapter profile

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

Before you begin

- The IBM Security Identity Governance and Intelligence server is installed and running.
- You have administrator authority on the IBM Security Identity Governance and Intelligence server.
- The file to be imported must be a Java archive (JAR) file. The <*Adapter*>Profile.jar file includes all the files that are required to define the adapter schema, account form, service/target form, and profile properties. If

necessary, you can extract the files from the JAR file, modify the files, and repackage the JAR file with the updated files.

About this task

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

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

Results

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

What to do next

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

- Import the attribute mapping file. See “Importing attribute mapping file” on page 12.

- Create a connector that uses the target profile. See "Adding a connector."

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

Adding a connector

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

Before you begin

Complete "Importing the adapter profile" on page 10.

Note: If you migrated from Identity Governance and Intelligence 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 Identity Governance and Intelligence 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 Identity Governance and Intelligence 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. 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 Identity Governance and Intelligence. For more information, see “Enabling connectors.”

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

Table 4. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Identity Governance and Intelligence.	"Adding a connector" on page 12.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 15.

Procedure

To enable a connector, complete these steps:

1. Log in to the Identity Governance and Intelligence 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 Identity Governance and Intelligence.

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 Identity Governance and Intelligence 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 Identity Governance and Intelligence V5.2.3:

1. Log in to the Identity Governance and Intelligence 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 13.

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

    For Identity Brokerage HR feed connectors, only the check box for enabling the read-from channel is available.
12. Start the connector by selecting **Monitor** > **Connector Status**. Select the connector that you want to start, and then select **Actions** > **Start**.

Attribute Mapping

Attribute mapping is required to define which target attributes correspond to the Identity Governance and Intelligence account attributes.

About this task

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

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

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

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

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

Note:

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

Procedure

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

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

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

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

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

```
Attribute   Mapped Attribute
eruid       CODE
erpassword  PASSWORD
```

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

Service/Target form details

Complete the service/target form fields.

Service Details

Service Name
Specify a name that defines the adapter service on the IIBM Security Identity Governance and Intelligence server.

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

Description
Specify a description that identifies the service for your environment.

IBM Tivoli Directory Integrator location
Specify the URL for the IBM Tivoli Directory Integrator instance.

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

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

Connection Details

Server URL
The CyberArk server URL. This field is mandatory.

For example, `http://<Instance name>:<Port number>`.

Login ID
The CyberArk user account login ID that adapter uses to connect to the CyberArk Server instance. This field is mandatory.

Password
Password for CyberArk user account. This field is mandatory.

Search Page Size (1-999)
[Optional] Specify a limit for the number of accounts to return for reconciliation.

Dispatcher Attributes

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

AL FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines that are received from IBM Security Identity Manager server. For example, you can specify the following file path to load the assembly lines from the profiles directory of the Windows operating system: `c:\Program Files\IBM\TDI\V7.1.1\profiles` or you can specify the following file path to load the assembly lines from the profiles directory of the UNIX and Linux operating: `system:/opt/IBM/TDI/V7.1.1/profiles`.

Max Connection Count
Specify the maximum number of assembly lines that the dispatcher can run simultaneously for the service. For example, enter 10 when you want the dispatcher to run maximum 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.

Status and information
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 to which the adapter is connected.

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

Profile version
Specifies the version of the profile that is installed in the IBM Security Identity Manager.

TDI version
Specifies the version of the IBM Tivoli Directory Integrator on which the adapter is deployed.

Dispatcher version
Specifies the version of the Dispatcher.

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

Adapter account
Specifies the account that 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 or perform the following verifications:

- 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. For example, verify the work station name or the IP address of the managed resource and the port.

Verifying that the adapter is working correctly

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

Procedure

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

Chapter 4. Upgrading

Upgrading an IBM Tivoli 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.

See the Release Notes for the supported software versions or for specific instructions.

Upgrading the Dispatcher

The new adapter package might require an upgrade of the Dispatcher.

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

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

Note: The Dispatcher installer stops the Dispatcher service before the upgrade and restarts it after the upgrade is complete.

Upgrading the adapter profile

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

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

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 the following configuration options:

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

Customizing the adapter profile

You can customize the adapter profile to change the account form or the service form. To customize the adapter profile, you must modify the adapter JAR file.

About this task

Use the Form Designer or the `CustomLabels.properties` file to change the labels on the forms. Each adapter has a `CustomLabels.properties` file.

The JAR file is included in the adapter package that you downloaded from the IBM Passport Advantage website. The JAR file and the files in the JAR file vary depending on your operating system.

The `adapter` profile JAR file includes the following files:

- `erCyberArkAccount.xml`
- `erCyberArkService.xml`
- `CyberArkSearch.xml`
- `CyberArkTest.xml`
- `CyberArkAdd.xml`
- `CyberArkModify.xml`
- `CyberArkDelete.xml`
- `schema.dsml`
- `service.def`
- `CustomLabels.properties`

Procedure

1. Edit the `JAR` file.
   a. Log on to the workstation where the CyberArk adapter is installed.
   b. On the **Start** menu, select **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. Type the name of the JAR file for your operating system. The following example applies to the CyberArk adapter profile.

```
cd c:\temp cd /tmp
jar -xvf CyberArkProfile.jar
```

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

e. Edit the file that you want to change.

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

2. Import the file.

a. Create a JAR file by using the files in the directory. Run the following commands:

Windows

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

UNIX

```
cd /tmp
jar -cvf CyberArkProfile.jar CyberArkProfile
```

b. Import the JAR file into the IBM Security Identity Governance and Intelligence application server.

c. Stop and start the IBM Security Identity server

d. Restart the adapter service.

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?

Logs

When the adapter is initially configured, a default directory is selected to store the log files that record the adapter activities. Logs can help you determine the background or cause of an issue and to find the proper solution.

```
<Log Level> [<Assembly Line_ProfileName>_<Request Id>]_
[<Connector Name>] - <message>
```

Log Level
Specifies the logging level that you configured for the adapter. The options are DEBUG, ERROR, INFO, and WARN. For information about using the `log4j.properties` file to configure logging, see the *Dispatcher Installation and Configuration Guide*.

Assembly Line
Specifies the name of the assembly line that is logging the information.

ProfileName
Specifies the name of the profile. Profile names can vary based on the adapter that is running or the operating system.

Request ID
Specifies the number of the request. The Request ID is used to uniquely identify a specific request.

Connector Name
Specifies the adapter connector.

Message
Specifies the informational message.

When you click the **Test** button on the CyberArk adapter service form, the service, environment, and configuration values are sent to the IBM Tivoli Directory Integrator log during the test. These collected information can help diagnose issues.

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.

The following table contains warnings or errors, which might be displayed when the CyberArk adapter is installed on your system.

Table 5. Specific warning and error messages and actions

Message	Action
Test Connection Fails: An error occurred while establishing communication with the Tivoli Directory Integrator server	• Verify that the IBM Tivoli Directory Integrator-based adapter service is running. • Verify that the URL specified on the service form for IBM Tivoli Directory Integrator is correct.

Table 5. Specific warning and error messages and actions (continued)

Message	Action
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again.	The service name might contain special characters that IBM Tivoli Directory Integrator can not handle. For example, "/".
Test Connection Fails: CTGIMU107W The connection to the specified service cannot be established. Verify the service information, and try again. **ibmdi.log** CTGDIS809E handleException - cannot handle exception , script java.lang.NoClassDefFoundError:	Verify that the file exists in the *ITDI_HOME*/jars/3rdparty/other: • httpclient-4.5.5.jar • httpcore-4.4.9.jar • jackson-annotations-2.5.0.jar • jackson-core-2.5.0.jar • jackson-databind-2.5.0.jar

Chapter 7. Uninstalling

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

Procedure

1. Stop the IBM Security Identity Governance and Intelligence Dispatcher Service.
2. Remove the CyberArk adapter JAR files.
   a. Delete `CyberarkConnector.jar` from the *`ITDI_HOME`*`/jars/connectors` directory.
   b. Delete the additional jars from `ITDI_HOME/jars/3rdparty/IBM`:
      - `httpclient-4.5.5.jar`
      - `httpcore-4.4.9.jar`
      - `jackson-annotations-2.5.0.jar`
      - `jackson-core-2.5.0.jar`
      - `jackson-databind-2.5.0.jar`

      Note: Ensure that none of the jars are being used for other adapters before deleting them.
3. Delete the adapter profile from the IBM Security Identity Governance and Intelligence server.

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

Chapter 8. Reference

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

Adapter attributes and object classes

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

The CyberArk adapter supports a standard set of attributes. The following tables shows the attributes in the **erCyberArkAccount** object class.

Table 6. Supported attributes

Manage Resource Attribute	Adapter Attribute	Description	Single/Multi Value	DataType	Required Attribute
username	**eruid**	User name/ID	Single	String	YES
firstName	**erCyberArkFirstName**	First name	Single	String	NO
lastName	**erCyberArkLastName**	Last name	Single	String	NO
middleName	**erCyberArkMiddleName**	Middle name	Single	String	NO
displayName	**erCyberArkDisplayName**	Display name	Single	String	NO
nickname	**erCyberArkNickName**	Nickname	Single	String	NO
Id	**erCyberArkUserId**	User ID	Single	String	NO
Entitlements	**erCyberArkEntitlement**	User entitlements	Multivalued	String	NO
Location	**erCyberArkLocation**	User Location	Single	String	NO
userType	**erCyberArkUserType**	USer Type	Single	String	NO
Emails	**erCyberArkOfficeEmail**	Office Email ID	Single	String	NO
Emails	**erCyberArkOtherEmail**	Other Email ID	Single	String	NO
Emails	**erCyberArkHomeEmail**	Home email ID	Single	String	NO
Groups	**erCyberArkGroupName**	User group	Multivalued	String	NO
Safe	**erCyberArkUserContainer**	User Safe	Multivalued	String	NO
PrivilegedData	**erCyberArkPrivData**	User Privileged Data	Multivalued	String	NO

Special CyberArk adapter attributes

ercyberarkentitlement

This attribute can be used to assign rights to CyberArk user account.

This attribute is a multi0value attribute and can have the following possible values:

- `Activate Users`
- `Safes Admin`
- `Users Admin`
- `Rules Admin`
- `Audit Admin`
- `Backup Admin`
- `Categories Admin`
- `Networks Admin`

- Reset Password
- Restore Admin

Adapter configuration properties

To set the IBM Tivoli Directory Integrator configuration properties for the operation of the CyberArk adapter, see the *Dispatcher Installation and Configuration Guide*.

Printed in USA