IBM Security Verify Governance Identity Manager

SDI-based IBM Security Privileged Identity Manager adapter Installation and Configuration Guide

Contents

Tables

Chapter 1. Overview

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

Adapters can be on the managed resource. The Identity server manages access to the resource by using your security system.

Adapters function as trusted virtual administrators on the target operating system. They do tasks such as:

- Reconciling users, groups, admin domains and accesses
- Adding and removing access memberships,and other administrative functions that are done manually

The adapter runs as a service, independently of whether you are logged on to the Identity server.

The IBM® Security Privileged Identity Manager adapter enables communication between the Identity server and the IBM Security Privileged Identity Manager server.

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.

Use the Preinstallation roadmap to prepare the environment..

Table 1. Preinstallation roadmap

Task	For more information, see
Verify that your environment meets the software and hardware requirements for the adapter.	"Prerequisites" on page 5
Obtain the installation software.	"Software downloads" on page 6.
Obtain the necessary information for the installation and configuration.	"Installation worksheet" on page 6.

Use the Installation and configuration roadmap to complete the actual installation and configuration of the adapter.

Table 2. Installation and configuration roadmap

Task	For more information, see
Install the dispatcher.	"Installing the dispatcher" on page 11.
Export and import the SSL certificate.	"Exporting and importing the SSL certificate" on page 11.
Install the connector.	"Installing the adapter binaries or connector" on page 12.
Verify the adapter installation.	"Verifying the adapter installation" on page 12.
Import the adapter profile into the Identity server.	Importing the adapter profile.
Create an adapter service.	Creating an adapter service.
Configure the adapter.	Chapter 6, "Configuring," on page 23.

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

Prerequisites

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

Table 3 on page 5 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 3. Prerequisites to install the adapter

Prerequisite	**Description**
Directory Integrator	• IBM Security 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 Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	Identity server Version 10.0
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
Security Directory Integrator adapters solution directory	A Security Directory Integrator adapters solution directory is a Security Directory Integrator work directory for IBM Security Verify Adapters. For more information, see the *Dispatcher Installation and Configuration Guide*.
IBM Security Privileged Identity Manager user	Must have administrator privileges.

The following table lists the requirements to run the IBM Security Privileged Identity Manager connector.

Table 4. IBM Security Privileged Identity Manager connector prerequisites

Requirement	Description	Task
Export and Import the SSL certificate	Export the SSL certificate from the managed resource and import it to the certificate authority (CA) certificates of the Security Directory Integrator Java virtual machine (JVM).	See "Exporting and importing the SSL certificate" on page 11.

Note: Set the environmental variable CLASSPATH to Java version 1.5 or later that is required for the adapter installation or upgrade.

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.0: Administrator Guide*.

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 Verify Governance Identity Manager 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 5. Required information to install the adapter

Required information	Description	Value

Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory that contains adapter JAR files. For example, the `jars/connectors` subdirectory contains the JAR file for the UNIX adapter.	If Security Directory Integrator is automatically installed with your IBM Security Verify Governance Identity Manager product, the default directory path for Security Directory Integrator is as follows:
		Windows:
		• For version 7.1.1:
		`*drive*\Program Files \IBM\TDI\V7.1.1`
		UNIX:
		• For version 7.1.1:
		`/opt/IBM/TDI/V7.1.1`

Table 5. Required information to install the adapter (continued)

Required information	Description	Value

Adapters solution directory	When you install the dispatcher, the adapter prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory is at:
		Windows:
		- For version 7.1.1:
		`drive\Program Files \IBM\TDI\V7.1.1\timsol`
		UNIX:
		- For version 7.1.1:
		`/opt/IBM/TDI/V7.1.1/timsol`

Chapter 3. Installing in the Verify Governance Identity Manager virtual appliance

For Verify Governance Identity Manager target management, you can install an IBM Security Verify Adapters or a custom adapter on the built-in Security Directory Integrator in the virtual appliance instead of installing the adapter externally. As such, there is no need to manage a separate virtual machine or system.

About this task

This procedure is applicable for a selected list of Identity Adapters. See the Identity Adapters product documentation at http://www.ibm.com/support/knowledgecenter/SSIGMP_1.0.0/com.ibm.itim_pim.doc/c_adapters_intro.htm to determine which adapters are supported in Identity Governance and Intelligence, and which can be installed on the virtual appliance.

All Identity Governance and Intelligence supported adapters can be installed externally on the virtual appliance. Depending on the adapter, an external Security Directory Integrator may be required.

See the corresponding *Adapter Installation and Configuration Guide* for the specific prerequisites, installation and configuration tasks, and issues and limitations. See the *Adapters Release Notes* for any updates to these references.

Procedure

1. Download the adapter package from the IBM Passport Advantage.
   For example, `Adapter-<Adaptername>.zip`.

   The adapter package includes the following files:

   Table 6. Adapter package contents

Files	Descriptions
`bundledefinition.json`	The adapter definition file. It specifies the content of the package, and the adapter installation and configuration properties that are required to install and update the adapter.
Adapter JAR profile	An Security Directory Integrator adapter always include a JAR profile which contains: • `targetProfile.json` – Service provider configuration – Resource type configuration – SCIM schema extensions – List of assembly lines • A set of assembly lines in XML files • A set of forms in XML files • Custom properties that include labels and messages for supported languages. Use the **Target Administration** module to import the target profile.

Table 6. Adapter package contents (continued)

Files	Descriptions
Additional adapter specific files	Examples of adapter specific files: • Connector jar files • Configuration files • Script files • Properties files The file names are specified in the adapter definition file along with the destination directory in the virtual appliance.

2. From the top-level menu of the **Appliance Dashboard**, click **Configure** > **SDI Management**.
3. Select the instance of the Security Directory Integrator for which you want to manage the adapters and click **Manage** > **SDI Adapters**

   The **SDI Adapters** window is displayed with a table that list the name, version, and any comments about the installed adapters.
4. On the **SDI Adapters** window, click **Install**.
5. On the **File Upload** window, click **Browse** to locate the adapter package and then click **OK**. For example, `Adapter-`*`<Adaptername>`*`.zip`.
6. Provide the missing 3rd party libraries when prompted.
   a) On the **File Upload** for Pre-requisite files window, click **Select Files**.

      A new **File Upload** window is displayed.

   b) Browse and select all the missing libraries. For example, `httpclient-4.0.1.jar`

   c) Click **Open**.

      The selected files are listed in the **File Upload** for Pre-requisite files window.

   d) Click **OK**.

      The missing files are uploaded and the adapter package is updated with the 3rd party libraries.
7. Enable secure communication.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Edit**.

   c) Click the **Enable SSL** check box.

   d) Click **Save Configuration**.
8. Import the SSL certificate to the IBM Security Directory Integrator server.
   a) Select the instance of the Security Directory Integrator for which you want to manage the adapter.

   b) Click **Manage** > **Certificates**.

   c) Click the **Signer** tab.

   d) Click **Import**.

      The **Import Certificate** window is displayed.

   e) Browse for the certificate file.

   f) Specify a label for the certificate. It can be any name.

   g) Click **Save**.

Chapter 4. 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 Installing the Dispatcher.

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*.

Exporting and importing the SSL certificate

To enable communication between the IBM Security Privileged Identity Manager adapter and the IBM Security Privileged Identity Manager server, keystores must be configured for the RMI Dispatcher.

Procedure

1. Create a keystore that contains the IBM Security Privileged Identity Manager SSL certificates as trusted certificate entries.

   Use Microsoft Internet Explorer to download the IBM Security Privileged Identity Manager server SSL certificate into the Windows certificate store from `{ISPIM Server IP/Hostname}`.

   View the certificate by double-clicking the **SSL lock** icon. If your browser reports that revocation information is not available, double-click **View Certificate**.
2. Click **Certification Path** and select the **CA Root** certificate.

   The Java™ keytool displays a confirmation that the certificate is added to the keystore.
3. Click **View Certificate**.
4. Click the **Details** tab and navigate to **Copy to File using the Base-64 encoded X.509 (.CER) format**.

   - If the RMI Dispatcher has the configured keystore, use the **`keytool.exe`** program to import the IBM Security Privileged Identity Manager server certificate.
   - If the keystore is not configured, create a keystore. Issue the following command (as one line) from a command prompt:

     ```
     keytool -import -alias ispim -file
     c:\ISPIM.cer -keystore c:\truststore.jks -storepass passw0rd
     ```
5. Edit the *`IDI_HOME`*`/timsol/solution.properties` file to specify truststore and keystore information.

   In the current release, only `jks-type` is supported:

   ```
   # Keystore file information for the server authentication.
   # It is used to verify the server's public key.
   ```

```
# example
javax.net.ssl.trustStore=truststore.jks
javax.net.ssl.trustStorePassword=passw0rd
javax.net.ssl.trustStoreType=jks
```

Note: If these key properties are not configured, you can set the truststore to the same value that contains the IBM Security Privileged Identity Manager server certificate. Otherwise, you must import the IBM Security Privileged Identity Manager server certificate to the truststore specified in `javax.net.ssl.trustStore`.

6. After you modify the `solution.properties` file, restart the IBM Security Verify Governance Identity Manager Adapter Service (RMI Dispatcher).

What to do next

For more information about SSL configuration, see the *IBM Security Dispatcher Installation and Configuration Guide*.

Installing the adapter binaries or connector

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

Before you begin

- The Dispatcher must be installed.

About this task

If you are updating a previous installation, the adapter you want to update must exist. If it does not exist, the software generates the following message:

```
Adapter is not found at specified location.
Cannot perform Update Installation. Correct
the path of installed adapter or select Full Installation.
```

Procedure

To install the adapter, take the following steps:

1. Create a temporary directory on the workstation where you want to install the adapter.
2. Extract the contents of the compressed file in the temporary directory.
3. Copy the `ISPIMConnector.jar` file to the *`ITDI_HOME`*`/jars/connectors` directory.
4. Download the `httpclient-4.0.1.jar` file from the Apache download page.
5. Copy the `httpclient-4.0.1.jar` file to the *`ITDI_HOME`*`/jars/3rdparty/others` directory.
6. Restart the adapter service.

Verifying the adapter installation

If the adapter is installed correctly, adapter components exist in the specified directory.

Table 7. Adapter component

Adapter component	**Directory**
`ISPIMConnector.jar`	*`ITDI_HOME`*`/jars/connectors`
`httpclient-4.0.1.jar`	*`ITDI_HOME`*`/jars/3rdparty/others`

Review the installer log file, `PIM_Installer.log`, that is in the adapter installer directory for any errors.

If this installation is to upgrade a connector, then send a request from IBM Security Verify Governance Identity Manager. Verify that the version number in the `ibmdi.log` matches the version of the connector that you installed. The `ibmdi.log` file is in the *`ITDI_Home`*`\`*`adapter solution directory`*`\logs` directory.

Restarting the adapter service

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

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

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

Importing the adapter profile

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

Before you begin

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

About this task

Target definition files are also called adapter profile files. The profile definition files are provided with the various IBM Security Verify Adapter. The adapter profile must be imported because it defines the types of resources that the Verify Governance 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.
- Create a connector that uses the target profile. See "Adding a connector" on page 16.

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.

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

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

Attribute Mapping

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

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.

Service/Target form details

Complete the service/target form fields.

General Information

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

Optionally, specify a description that identifies the service for your environment.

Server URL

Specify the base URL for the IBM Security Privileged Identity Manager.

Security Directory Integrator location

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

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

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

Table 8. Ports

Instance	Ports
SDI1	1199, 1198, 1197, 1196, 1195, 1194
SDI2	2299, 2298, 2297, 2296, 2295, 2294
SDI3	3399, 3398, 3397, 3396, 3395, 3394
SDI4	4499, 4498, 4497, 4496, 4495, 4494
SDI5	5599, 5598, 5597, 5596, 5595, 5594
SDI6	6699, 6698, 6697, 6696, 6695, 6694
SDI7	7799, 7798, 7797, 7796, 7795, 7794
SDI8	8899, 8898, 8897, 8896, 8895, 8894
SDI9	9999, 9998, 9997, 9996, 9995, 9994
SDI10	11099, 11098, 11097, 11096, 11095, 11094

For a high availability implementation, use any of these port numbers.

- 1099
- 2099
- 3099

Owner
Optionally, specify a user as a service owner.

Service Prerequisite
Optionally, specify a service that is prerequisite to this service.

Authentication

Administrator name

Specify the name of a user with administrative privileges on the IBM Security Privileged Identity Manager server.

Password

Specify the password for the administrator.

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

Chapter 5. Upgrading

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

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

Upgrading the adapter binaries or connector

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

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

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

Upgrading the adapter profile

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

Chapter 6. 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 to support custom attributes

Use these tasks to configure the IBM Security Privileged Identity Manager adapter to support customized IBM Security Privileged Identity Manager attributes.

IBM Security Privileged Identity Manager supports custom fields for the user object. However, the IBM Security Privileged Identity Manager adapter supports only the standard set of attributes.

You can customize the adapter to support custom attributes. Complete the following tasks to customize the IBM Security Privileged Identity Manager adapter to support custom fields in IBM Security Privileged Identity Manager.

Related concepts

Modifying the maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

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.

Creating a JAR file and importing the profile into the Identity server
After you modify the `schema.dsml` or any other profile files, you must import these files, into IBM Security Verify Governance Identity Manager for the changes to take effect.

Schema extensions and custom attributes

Use the interface and tools that are provided by IBM Security Privileged Identity Manager to extend the IBM Security Privileged Identity Manager user schema and add the custom attributes.

For more information about adding new attributes to the IBM Security Privileged Identity Manager User schema, see the IBM Security Privileged Identity Manager documentation.

The IBM Security Privileged Identity Manager adapter supports the following types of custom attributes:

- Boolean
- Integer
- Case-sensitive string
- Not case-sensitive string
- Coordinated Universal Time (UTC) coded time

Prefix the attribute names with `erPIM` to easily identify the attributes that are used with IBM Security Verify Governance Identity Manager.

Note:

- If Security Directory Server is being used as the directory server application, the name of the attribute must be unique within the first 16 characters.
- The IBM Security Privileged Identity Manager adapter supports a multi-line value for custom attributes with string syntax.
- The custom attributes are supported for User account class only.

Related concepts

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the IBM Security Privileged Identity Manager adapter forms to use the new custom attributes.

Related tasks

Copying the adapter file and extracting the files
Use these tasks to customize your environment.

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

Updating the schema.dsml file
The IBM Security Privileged Identity Manager adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the IBM Security Privileged Identity Manager adapter form.

Creating a JAR file and installing the new attributes on the Identity server
You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Copying the adapter file and extracting the files

Use these tasks to customize your environment.

About this task

The profile JAR file, `ISPIMProfile.jar`, is included in the IBM Security Privileged Identity Manager adapter compressed file that you downloaded from the IBM website. The `ISPIMProfile.jar` file contains a folder named `ISPIM profile` with the following files:

- `CustomLabels.properties`
- `erISPIMAccess.xml`
- `erISPIMAccount.xml`
- `erISPIMDomain.xml`
- `erISPIMGroup.xml`
- `erISPIMService.xml`
- `ispimAccessModify.xml`
- `ispimAdminDomainModify.xml`
- `ispimGroupModify.xml`
- `ispimRecon.xml`
- `ispimTest.xml`
- `ispimUserAdd.xml`

- `ispimUserModify.xml`
- `schema.dsml`
- `service.def`

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

Procedure

1. Log in to the system where the IBM Security Privileged Identity Manager adapter is installed.
2. On the **Start** menu, click **Programs** > **Accessories** > **Command Prompt**.
3. Copy the `ISPIMProfile.jar` file into a temporary directory.
4. Extract the contents of` the `ISPIMProfile.jar` file into the temporary directory.

   Run the following commands:

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

   The **`jar`** command creates the `c:\temp\ISPIM profile` directory.

What to do next

Edit the appropriate files by completing the following tasks.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by IBM Security Privileged Identity Manager to extend the IBM Security Privileged Identity Manager user schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the IBM Security Privileged Identity Manager adapter forms to use the new custom attributes.

Related tasks

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

Updating the schema.dsml file
The IBM Security Privileged Identity Manager adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the IBM Security Privileged Identity Manager adapter form.

Creating a JAR file and installing the new attributes on the Identity server
You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Modifying the assembly lines

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

About this task

The IBM Security Privileged Identity Manager adapter uses Security Directory Integrator to process requests before you submit them to IBM Security Privileged Identity Manager.

The IBM Security Privileged Identity Manager assembly lines contain mapping instructions from a IBM Security Verify Governance Identity Manager request to IBM Security Privileged Identity Manager. Modify the assembly lines to add new mappings for custom attributes.

Procedure

1. Start the Tivoli Directory Integrator Configuration Editor.
2. Open the `ispimUserAdd.xml` file. Click **File** > **Open Tivoli Directory Integrator Configuration File...**.
    a) Browse to the `ISPIM profile` directory.
    b) Select the `ispimRecon.xml` file.
3. Optional: If previously edited, assign this configuration file to an existing project. Otherwise, proceed to the next screen to create a project and name it `ISPIMProfile`.
4. After the file is imported, expand the project to display the **AssemblyLines** tree in the Navigator pane.
5. Right click **pimRecon assemblyline** and select **Open**. The Recon assemblyline configurations are displayed in the main panel.
6. Click **Show Mapping** in the main panel. The mapping table for the assembly line is displayed in the main panel.
7. Locate the **ReconUser** section and left click to select it in the table.
8. Click **Map** to display the Add attribute dialog.
9. Enter the name of the custom field exactly as displayed in the API Name on IBM Security Privileged Identity Manager.
    For example, `Custom1__c`.
10. After the field is added, locate it in the mapping table and double-click the corresponding row to display an edit dialog.
11. Change the default value of `work.[custom field name]` to `work.[custom attribute name]`.
    For example, change `work.Custom1__c` to `work.erISPIMCustom1_c`.
12. Save the changes. Click **File** > **Save**.
13. Right click the project in the Navigator pane and select the **Export...** option to export the new assembly line.
14. In the first screen of the **Export** dialog, expand the IBM Security Directory Integrator folder and select **Runtime Configuration**.
15. Click **Next**.
16. In the file path field, browse to the `ISPIM profile` directory and select the file with the same name from step 2 to overwrite it.
17. Click **Finish**.
18. Repeat the steps 5 through 17 for the Modify assembly line.
19. Repeat steps 5 through 17 for the Recon assembly line and do the following steps instead of steps 10 and 11:
    a) Locate the field in the mapping table and click the **Work Attribute** cell corresponding to the custom field to rename it.
    b) Enter the attribute name that is specified previously in step 11.
    For example, `erISPIMCustom1_c`.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by IBM Security Privileged Identity Manager to extend the IBM Security Privileged Identity Manager user schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the IBM Security Privileged Identity Manager adapter forms to use the new custom attributes.

Related tasks

Copying the adapter file and extracting the files

Use these tasks to customize your environment.

Updating the schema.dsml file
The IBM Security Privileged Identity Manager adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the IBM Security Privileged Identity Manager adapter form.

Creating a JAR file and installing the new attributes on the Identity server
You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Updating the `schema.dsml` file

The IBM Security Privileged Identity Manager adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

About this task

For more information about the attributes in this file, see "The schema.dsml file" on page 35.

Procedure

1. Locate the `schema.dsml` file in the `ISPIM profile` directory.
2. Edit the `schema.dsml` file to add an attribute definition for each custom attribute.

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

   For example, if the last attribute in the file uses the OID 1.3.6.1.4.1.6054.3.182.2.47, the first new attribute uses the OID 1.3.6.1.4.1.6054.3.182.2.48.

   You might want to start a new range of numbers for your custom attributes. For example, start custom attributes with OID 11.3.6.1.4.1.6054.3.176.2.1000. This range prevents duplicate OIDs if the adapter is upgraded to support new attributes that are standard for newer versions of IBM Security Privileged Identity Manager API.
3. Add each of the new attributes to the account class.
   For example, add the following attribute definition under the `erPIMAccount` section of the `schema.dsml` file:

   ```
   <attribute ref="erISPIMCustom1_c" required="false"/>
   ```
4. Save the file when you are finished.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by IBM Security Privileged Identity Manager to extend the IBM Security Privileged Identity Manager user schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the IBM Security Privileged Identity Manager adapter forms to use the new custom attributes.

Related tasks

Copying the adapter file and extracting the files
Use these tasks to customize your environment.

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

Modifying the CustomLabels.properties file

After you add the custom attributes to the schema.dsml file, the attributes are available for use on the IBM Security Privileged Identity Manager adapter form.

Creating a JAR file and installing the new attributes on the Identity server
You must import the modified assembly lines, schema.dsml, CustomLabels.properties, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Modifying the CustomLabels.properties file

After you add the custom attributes to the schema.dsml file, the attributes are available for use on the IBM Security Privileged Identity Manager adapter form.

About this task

The attributes are displayed in the attribute list for the account form. You can modify the attribute names that are in the attribute list. See "CustomLabels.properties file" on page 38.

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

Procedure

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

   Use the following format:

   ```
   attribute=label
   ```

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

   ```
   #
   Adapter Labels definitions
   #
   erISPIMCustom1_c=Custom Field One
   erISPIMCustom2_c=Custom Attribute Field Two
   ```

3. Save the file when you are finished.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by IBM Security Privileged Identity Manager to extend the IBM Security Privileged Identity Manager user schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the IBM Security Privileged Identity Manager adapter forms to use the new custom attributes.

Related tasks

Copying the adapter file and extracting the files
Use these tasks to customize your environment.

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

Updating the schema.dsml file
The IBM Security Privileged Identity Manager adapter schema.dsml file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Creating a JAR file and installing the new attributes on the Identity server

You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Creating a JAR file and installing the new attributes on the Identity server

You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

Procedure

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

   Run the following commands:

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

2. Import the `ISPIMProfile.jar` file into the Identity server.

   For more information about importing the file, see Importing the adapter profile.

3. Start and stop the Identity server.

   Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the Identity server to refresh the cache and the adapter schema. See Chapter 5, “Upgrading,” on page 21.

Related concepts

Schema extensions and custom attributes
Use the interface and tools that are provided by IBM Security Privileged Identity Manager to extend the IBM Security Privileged Identity Manager user schema and add the custom attributes.

Adapter form modification (optional)
After the changes are available in the Identity server, you can modify the IBM Security Privileged Identity Manager adapter forms to use the new custom attributes.

Related tasks

Copying the adapter file and extracting the files
Use these tasks to customize your environment.

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

Updating the schema.dsml file
The IBM Security Privileged Identity Manager adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the IBM Security Privileged Identity Manager adapter form.

Adapter form modification (optional)

After the changes are available in the Identity server, you can modify the IBM Security Privileged Identity Manager adapter forms to use the new custom attributes.

You do not have to add the attributes to the IBM Security Privileged Identity Manager adapter form unless you want them to be available. The attributes are returned during reconciliations unless you explicitly exclude them.

Related concepts

Schema extensions and custom attributes

Use the interface and tools that are provided by IBM Security Privileged Identity Manager to extend the IBM Security Privileged Identity Manager user schema and add the custom attributes.

Related tasks

Copying the adapter file and extracting the files
Use these tasks to customize your environment.

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

Updating the schema.dsml file
The IBM Security Privileged Identity Manager adapter `schema.dsml` file identifies all of the standard User account attributes. Modify this file to identify new custom attributes.

Modifying the CustomLabels.properties file
After you add the custom attributes to the `schema.dsml` file, the attributes are available for use on the IBM Security Privileged Identity Manager adapter form.

Creating a JAR file and installing the new attributes on the Identity server
You must import the modified assembly lines, `schema.dsml`, `CustomLabels.properties`, and any other files in the profile that were modified for the adapter. The changes do not take effect until after the files are imported into the Identity server.

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 concepts

Customizing the adapter to support custom attributes
Use these tasks to configure the IBM Security Privileged Identity Manager adapter to support customized IBM Security Privileged Identity Manager attributes.

Modifying the maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

Related tasks

Creating a JAR file and importing the profile into the Identity server

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

Modifying the maximum length of the account form attributes

When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

For example, when you want 2048 as the maximum length of the **`First Name`** attribute, modify the `schema.dsml` file as:

```
Old profile:

<!-- ******************************************************** -->
<!-- erISPIMFirstName -->
<!-- ********************************************************
--> <attribute-type single-value="true">
            <name>erISPIMFirstName</name>
            <description>The first name field of an ISPIM user account</description>
            <object-identifier>1.3.6.1.4.1.6054.3.182.2.4</object-identifier>
            <syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
  </attribute-type>

Modified profile:

<!-- ******************************************************** -->
<!-- erISPIMFirstName -->
<!-- ********************************************************
--> <attribute-type single-value="true">
            <name>erISPIMFirstName</name>
            <description>The first name field of an ISPIM user account</description>
            <object-identifier>1.3.6.1.4.1.6054.3.182.2.4</object-identifier>
            <syntax>1.3.6.1.4.1.1466.115.121.1.15{2048}</syntax>
  </attribute-type>
```

Related concepts

Customizing the adapter to support custom attributes
Use these tasks to configure the IBM Security Privileged Identity Manager adapter to support customized IBM Security Privileged Identity Manager attributes.

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.

Creating a JAR file and importing the profile into the Identity server
After you modify the `schema.dsml` or any other profile files, you must import these files, into IBM Security Verify Governance Identity Manager for the changes to take effect.

Creating a JAR file and importing the profile into the Identity server

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

About this task

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. You must stop and start the Identity server to refresh the cache and the adapter schema. For more information about upgrading an existing adapter, see Chapter 5, “Upgrading,” on page 21.

Procedure

1. Extract the contents of the `ISPIMProfile.jar` file into the temporary directory by running the following command:

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

The **jar** command creates the `c:\temp\ISPIM profile` directory.

2. Update the profile files.
3. Create a JAR file with the files in the `\temp` directory by running the following commands:

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

4. Import the `ISPIMProfile.jar` file into the Identity server.

   For more information about importing the file, see Importing the adapter profile.
5. Stop and start the Identity server.

Related concepts

Customizing the adapter to support custom attributes
Use these tasks to configure the IBM Security Privileged Identity Manager adapter to support customized IBM Security Privileged Identity Manager attributes.

Modifying the maximum length of the account form attributes
When you want to modify the maximum length of the attributes on the account form, modify the `schema.dsml` file with their required length.

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.

Chapter 7. Uninstalling

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

Removing the adapter binaries or connector

The IBM Security Privileged Identity Manager adapter installation installs the Security Directory Integrator IBM Security Privileged Identity Manager connector.

About this task

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

Procedure

1. Stop the Dispatcher service.
2. Remove the `ISPIMConnector.jar` file from *`ITDI_HOME`*`/jars/connectors` directory.
3. Start the Dispatcher service.

Deleting the adapter profile

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

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

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

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

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

Files

You can configure several adapter-specific files that are associated with the IBM Security Privileged Identity Manager adapter.

- "The schema.dsml file" on page 35
- "CustomLabels.properties file" on page 38

The `schema.dsml` file

The `schema.dsml` file contains all of the attributes that are common to all adapters. This common file also contains Identity server attributes that can be used by any adapter. The `schema.dsml` file defines all of the classes that are used by the adapter. The classes are used to declare accounts, services, and supporting data.

The `schema.dsml` file defines the attributes and objects that the adapter supports and uses to communicate with the Identity server. All attributes must be unique. Therefore, they are assigned an object identifier (OID).

The OID is defined with the `<object-identifier>...</object-identifier>`

The `schema.dsml` file has the following format:

```
SCHEMA.DSML File<?xml version="1.0" encoding="UTF-8"?>
<dsml>
<!-- ******************************************************** -->
<!-- Schema supported by the IBM Security Privileged Identity Manager adapter. -->
<!-- ******************************************************** -->
<directory-schema> ...
<!-- ******************************************************** -->
<!-- erISPIMString1-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erISPIMString1</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.182.2.100</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erISPIMInteger-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erISPIMInteger</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.182.2.101</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.27</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erISPIM-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erISPIMDate</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.182.2.102</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.24</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erISPIMBoolean-->
<!-- ******************************************************** -->
<attribute-type single-value="true">
<name>erISPIMBoolean</name>
<description/>
<object-identifier>1.3.6.1.4.1.6054.3.182.2.103</object-identifier>
```

```
<syntax>1.3.6.1.4.1.1466.115.121.1.7</syntax>
</attribute-type>
<!-- ******************************************************** -->
<!-- erISPIMMultiValueString-->
<!-- ******************************************************** -->
<attribute-type>
<name>erISPIMMultiValueString</name>
<description>List of string values</description>
<object-identifier>1.3.6.1.4.1.6054.3.182.2.104</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type> ...
<!-- ******************************************************** -->
<!-- erISPIMAccount -->
<!-- ******************************************************** -->
<class superior="top">
<name>erISPIMAccount</name>
<description>Class representing a PIM account.</description> ...
<object-identifier>1.3.6.1.4.1.6054.3.182.1.1</object-identifier>
<attribute ref="erPIMBoolean" required="false"/>
<attribute ref="erPIMDate" required="false"/>
<attribute ref="erPIMInteger" required="false"/>
<attribute ref="erPIMMultiValueString" required="false"/>
<attribute ref="erPIMString1" required="false"/>
</class> ...
</directory-schema>
</dsml>
```

Object identifier

The Identity server uses LDAP directory services to add, delete, modify, and search IBM Security Verify Governance Identity Manager data. Each data item in an LDAP directory server must have a unique object identifier (OID). Therefore, each attribute and class that is defined in the `schema.dsml` file in IBM Security Verify Governance Identity Manager has an OID.

OIDs have the following syntax:

```
enterprise ID.product ID.adapter ID.object ID.instance ID
```

- The *enterprise ID* is always 1.3.6.1.4.1.6054 for IBM.
- The *product ID* is always 3 because these `schema.dsml` files are used with adapters.
- The *adapter ID* is 182 for the IBM Security Privileged Identity Manager adapter.
- The *object ID* is 2. An attribute uses 2 as the object ID.
- The *instance ID* is a sequential number of the object.

Attribute definition

Before you define unique attributes for the adapter, ensure that the attribute does not exist in the common `schema.dsml` file.

The following example defines an attribute:

```
<!-- ********************************************** -->
<!-- erSampleHome -->
<!-- ********************************************** -->
<attribute-type single-value = "true" >
<name>erSampleHome</name>
<description>User home directory</description>
<object-identifier>1.3.6.1.4.1.6054.3.125.2.100</object-identifier>
<syntax>1.3.6.1.4.1.1466.115.121.1.15</syntax>
</attribute-type>
```

Comment lines are denoted by the `<!-- ... -->` markers

The attribute type is defined as single-value or multi-value. A single-value attribute is denoted by the line: `<attribute-type single-value ="true">`. To denote a multi-valued attribute, change the `true` value to `false`.

The name of the attribute that is used by the Identity server is defined in the schema. To simplify the tracking of new IBM Security Privileged Identity Manager adapter attributes, use `erPIM` as the preface for all new attributes.

The description of the attribute is denoted by the line: `<description>...</description>` tag.

The OID is defined by the `<object-identifier>...</object-identifier>` tag. Because OIDs are already assigned to the existing, standard attributes, the OID can be copied from the last attribute in the list. However, the last number must be incremented by one for each new attribute that you add to the `schema.dsml` file.

The data type is defined with the `<syntax>...</syntax>` tag. The following table lists various data types and the value you specify in the syntax tags.

Table 9. Syntax tag data types and values

Data type	Value
Bit string	1.3.6.1.4.1.1466.115.121.1.6
Boolean	1.3.6.1.4.1.1466.115.121.1.7
Directory string	1.3.6.1.4.1.1466.115.121.1.15
UTC coded time	1.3.6.1.4.1.1466.115.121.1.24
Integer	1.3.6.1.4.1.1466.115.121.1.27

Classes

At least one account class and one service class must be defined in the `schema.dsml` file.

Each class requires at least one attribute to identify the class: a name attribute. More attributes might be required depending on the class that is defined.

The following syntax defines a class:

```
<class superior="top">
<name> ... </name>
<description> ... </description>
<object-identifier> ... </object-identifier>
<attribute ref = "..." required = "true" />
<attribute ref = "..." required = "true" />
</class>
```

To make an attribute optional for a class, change `required = "true"` to `required = "false"` in the <attribute ref> tag.

An account class defines the attributes that are used to describe an account. An account class must be defined in the `schema.dsml` file.

The following example defines an account class:

```
<class superior="top" >
<name>erSampleAccount</name>
<description>Sample Account</description>
<object-identifier>1.3.6.1.4.1.6054.3.125.1.101</object-identifier>
<attribute ref = "eruid" required = "true" />
<attribute ref = "erAccountStatus" required = "false" />
<attribute ref = "erSampleGroups" required = "false" />
<attribute ref = "erSampleHome" required = "false" />
<attribute ref = "erSampleDesc" required = "false" />
<attribute ref = "erPassword" required = "false" />
</class>
```

In the preceding example, the class name is erSampleAccount and the only required attribute is eruid. However, erAccountStatus is a required attribute to suspend or restore accounts.

`CustomLabels.properties` file

The `CustomLabels.properties` file is a text file that defines the labels on the form for the adapter.

Use this syntax for the information in the file:

```
attribute=text
```

where:

- *attribute* is the same attribute that is defined in the `schema.dsml` file.
- *text* is the label that is on the form in the IBM Security Verify Governance Identity Manager user interface for the account.

The value of *attribute* must be in lowercase. This requirement is from the Identity server.

Adapter attributes

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

As part of the adapter implementation, a dedicated account for IBM Security Verify Governance Identity Manager to access the IBM Security Privileged Identity Manager is created on the IBM Security Privileged Identity Manager. 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 IBM Security Privileged Identity Manager adapter with attributes that are included in transmission packets that are sent over a network.

The combination of attributes, included in the packets, depends on the type of action that the Identity server requests from the IBM Security Privileged Identity Manager adapter.

Table 10 on page 38 lists the attributes that are used by the IBM Security Privileged Identity Manager adapter. The table provides a description and the corresponding values of the attribute.

Use this key for the permissions column.

```
R = Read only
RW = Add, read, modify, write
AR = Add, Read
```

Table 10. Attributes for the erPIMAccount object class

Attribute name and defination	Data Type	Single-valued	Permissions	Required
erISPIMParentBusinessUnit	String	TRUE	R	TRUE
erUid	String	TRUE	R	TRUE
erISPIMChangePassword	String	TRUE	R	FALSE
erISPIMLastName	String	TRUE	R	TRUE
erISPIMFullName	String	TRUE	R	TRUE
erISPIMFirstName	String	TRUE	R	FALSE
erISPIMInitials	String	TRUE	R	FALSE
erISPIMHomeAddress	String	TRUE	R	FALSE
erISPIMSharedSecret	String	TRUE	R	FALSE
erISPIMOrgRoles	String	FALSE	RW	FALSE
erISPIMOfficeNumber	String	TRUE	R	FALSE
erISPIMEmployeeNumber	String	TRUE	R	FALSE

Table 10. Attributes for the erPIMAccount object class (continued)

erISPIMTitle	String	TRUE	R	FALSE
erISPIMManager	String	TRUE	R	FALSE
erISPIMPostalAddress	String	TRUE	R	FALSE
erISPIMAdminAssistant	String	TRUE	R	FALSE
erISPIMEmailAddress	String	TRUE	R	FALSE
erISPIMPhoneNumber	String	TRUE	R	FALSE
erISPIMMobileNumber	String	TRUE	R	FALSE
erISPIMPager	String	TRUE	R	FALSE
erISPIMHomePhoneNumber	String	TRUE	R	FALSE
erISPIMGroups	String	FALSE	R	FALSE
erISPIMAdminDomains	String	FALSE	R	FALSE
erAccountStatus	String	TRUE	R	FALSE
erPassword	String	TRUE	R	FALSE
erISPIMGlobalID	String	TRUE	R	FALSE
erISPIMUserId	String	TRUE	R	FALSE
erISPIMConstraintsRef	String	TRUE	R	FALSE
erISPIMSystemUser	String	TRUE	R	FALSE
erISPIMPersonRef	String	TRUE	R	FALSE
erISPIMManagerRef	String	TRUE	R	FALSE
erISPIMParentBusinessUnitRef	String	TRUE	R	FALSE
erISPIMUserPreferencesRef	String	TRUE	R	FALSE
erISPIMAdminDomainsRef	String	TRUE	R	FALSE
erISPIMSystemUserRef	String	TRUE	R	FALSE
erISPIMSelfRef	String	TRUE	R	FALSE

Index