IBM Security Identity Governance and Intelligence

IBM Security Access Manager Adapter Installation and Configuration Guide

IBM Security Identity Governance and Intelligence

IBM Security Access Manager 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 IBM Security Access Manager Adapter uses the IBM Tivoli® Directory Integrator function to facilitate communication between the IBM Security Identity server and IBM Security Access Manager Server.

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

Features of the adapter

The adapter automates several administrative and management tasks.

You can use the IBM Security Access Manager Adapter to automate the following account management tasks:

- Creating new users.
- Creating SSO credentials for users.
- Modifying users' SSO credentials and attributes.
- Changing user account passwords.
- Suspending, restoring, and deleting user accounts.
- Reconciling user, SSO credentials, and user attributes.
- Creating and deleting groups, and modifying their descriptions

Architecture of the adapter

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

You can do the following actions on an account:

- Add
- Delete
- Modify
- Change Password
- Restore
- Suspend
- Search for account information

The IBM Security Access Manager Adapter consists of IBM Tivoli Directory Integrator AssemblyLines. When an initial request is made by IBM Security Identity server to the IBM Security Access Manager Adapter, the AssemblyLines are loaded into the IBM Tivoli Directory Integrator server. As a result, subsequent service requests do not require those same AssemblyLines to be reloaded.

The AssemblyLines use the IBM Tivoli Directory Integrator IBM Security Access Manager connector and IBM Security Access Manager User connector to undertake user management-related tasks on the directory server. It does these tasks remotely by using the login user ID and password of a user that has administrator privileges.

Figure 1 shows the various components that work together to complete user management tasks in an IBM Tivoli Directory Integrator environment.

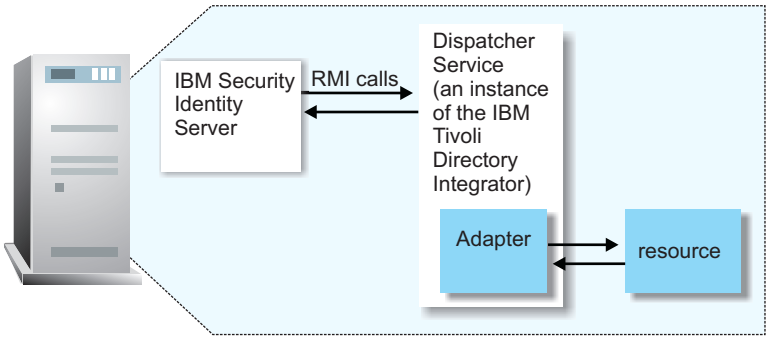

Figure 1. The architecture of the IBM Security Access Manager Adapter

For more information about IBM Tivoli Directory Integrator, see the *IBM Tivoli Directory Integrator: Getting Started Guide*.

Supported configurations

The IBM Security Access Manager Adapter supports a number of different configurations.

There are fundamental components of an IBM Security Access Manager Adapter environment:

- An IBM Security Identity server
- An IBM Tivoli Directory Integrator server
- A compatible directory server
- The IBM Security Access Manager Adapter.

The IBM Security Access Manager Runtime for Java™ Environment must also be configured on the same Java Runtime Environment (JRE) as used by IBM Tivoli Directory Integrator.

The IBM Security Access Manager Adapter is both highly configurable and highly customizable. Support can extend only to the configuration of the adapter such as adding mapping for more attributes. Support cannot extend to customization by way of changes, additions, or modifications to its IBM Tivoli Directory Integrator Assembly Line scripts for example.

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 hardware, software, and authorization prerequisites to install the IBM Security Access Manager Adapter.

Table 1. Prerequisites to install the adapter

Prerequisite	Description
Operating System	The IBM Security Access Manager Adapter can be used on any operating system that is supported by IBM Tivoli Directory Integrator.
Network Connectivity	TCP/IP network
System Administrator Authority	The person who completes the IBM Security Access Manager Adapter installation procedure must have system administrator authority to complete the steps.

Table 1. Prerequisites to install the adapter (continued)

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 + FP0002 + 7.2.0-ISS-SDI-LA0008 **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 Manager server Version 6.0 • IBM Security Identity Manager server Version 7.0 • IBM Security Privileged Identity Manager Version 2.0 • IBM Security Identity Governance and Intelligence server Version 5.2.2
IBM Security Access Manager	• Version 7.0.0-FP5 • Version 8.0.0-FP4 • Version 8.0.1-FP1 • Version 9.0.0-FP1
Dispatcher	Obtain the dispatcher installer from the IBM Passport Advantage® website: http://www-01.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
IBM Security Access Manager Java Runtime (previously known as IBM Tivoli Access Manager)	Corresponding version to the IBM Security Access Manager Server. The IBM Security Access Manager Adapter supports IBM Security Access Manager versions 7.0, 8.0, 8.01, and 9.0.

For information about the minimal system requirements and supported operating systems for IBM Tivoli Directory Integrator, refer to the *IBM Tivoli Directory Integrator: Administrator Guide*.

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 on page 6 identifies the information that you use to install the IBM Security Access Manager Adapter.

Table 2. Required information to install the adapter

Required information	Description
Administrator account on the managed resource for running the IBM Security Access Manager Adapter.	An administrator account on the managed resource that has administrative rights.
IBM Security Access Manager Administrator account	An administrator account in IBM Security Access Manager with administrative rights. For example, sec_master.

The IBM Security Access Manager Adapter distribution package contains the following adapter profile:

itamprofile.jar

The `itamprofile.jar` profile is used when IBM Security Access Manager is configured against supported LDAP and Active Directory user registries, including Active Directory Application Mode (ADAM) or other supported user registries.

Note: For an IBM Security Identity Governance and Intelligence installation that uses Sun Directory Server, use `itamprofileSunDS.jar` to install the profile.

It extends IBM Security Identity Governance and Intelligence directory schema with:

- IBM Security Access Manager account attributes
- Attributes from the **InetOrgPerson** object class as define in *RFC 2798 "Definition of the inetOrgPerson LDAP Object Class"*
- Attributes that can be mapped to Active Directory attributes

See Table 7 on page 29.

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.

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 the adapter binaries or connector

About this task

Procedure

Configuring the IBM Security Access Manager Run Time for Java System

The Java Run Time component (JRTE) must be installed on the same system where IBM Tivoli Directory Integrator Server and IBM Security Identity Adapter are installed.

About this task

For more information about installing the JRTE, see the *IBM Security Access Manager: Install Guide*.

To configure JRTE against IBM Tivoli Directory Integrator Server JRE, follow these configuration steps:

Procedure

1. Start the IBM Security Access Manager configuration utility. Run the command `pdconfig`
2. Select **Access Manager Runtime for Java** from the list of installed packages.
3. Click **Configure**.
4. Select **Full** for configuration type and then click **Next**.
5. Specify the JRE path such as `C:\Program Files\ibm\TDI\V7.1\jvm\jre`. Then, click **Next**.

6. Specify **Host name**, **Port**, and **Domain**. Then, click **Next**.
7. Optionally enable Tivoli Common logging. Then, click **Finish**. A message that states that JRTE is successfully configured is shown on the screen.
8. Click **Close** to exit the utility.

What to do next

For more information, see the *IBM Security Access Manager: Command Reference*.

Configuring the IBM Security Access Manager Registry Direct API for Java System

You must use the Registry Direct API to improve the adapter performance.

Procedure

Copy the `com.tivoli.pd.rgy.jar` file from IBM Security Access Manager installation directory to IBM Tivoli Directory Integrator JRE installation directory. On a Linux IBM Security Access Manager system, the `com.tivoli.pd.rgy.jar` file is typically at:

```
/opt/PolicyDirector/java/export/rgy
```

Copy this file to the following directory on the system where IBM Tivoli Directory Integrator is installed:

```
/opt/IBM/TDI/V7.1/jvm/jre/lib/ext
```

For more information, see Appendix D. Registry Direct Java API in the *IBM Security Access Manager: Administration Java Classes Development Reference*.

Configuring the IBM Tivoli Directory Integrator Java Runtime Environment into the IBM Security Access Manager secure domain

To use IBM Security Access Manager security, the IBM Security Identity Manager adapter must be configured into your IBM Security Access Manager secure domain.

About this task

IBM Security Access Manager provides a utility class `com.tivoli.pd.jcfg.SvrSslCfg` that can be used for configuration and unconfiguration tasks.

You must use the IBM Tivoli Directory Integrator JRE to run the utility.

For example, use the following command to configure the IBM Tivoli Directory Integrator to use the Registry Direct API to connect to IBM Security Access Manager with standard ports and default installation paths:

```
/opt/IBM/TDI/V7.1/jvm/jre/bin/java com.tivoli.pd.jcfg.SvrSslCfg
-action config
-admin_id sec_master
-admin_pwd SEC_MASTER_PASSWORD
-appsvr_id itdi_tam
-port 1234
-mode remote
-policysvr amserver.example.com:7135:1
```

```
-authzsvr amserver.example.com:7136:1
-cfg_file /opt/IBM/TDI/V7.1/timsol/tam.conf
-key_file /opt/IBM/TDI/V7.1/timsol/tam.ks
-ldap_mgmt true
-ldap_svrs ldapserver:389:readwrite:5
-ldap_ssl_enable false
```

To set up a slower Administration API for IBM Security Access Manager, use the following command:

```
/opt/IBM/TDI/V7.1/jvm/jre/bin/java com.tivoli.pd.jcfg.SvrSslCfg
  -action config
  -admin_id sec_master
  -admin_pwd SEC_MASTER_PASSWORD
  -appsvr_id itdi_tam
  -port 1234
  -mode remote
  -policysvr amserver.example.com:7135:1
  -authzsvr amserver.example.com:7136:1
  -cfg_file /opt/IBM/TDI/V7.1/timsol/tam.conf
  -key_file /opt/IBM/TDI/V7.1/timsol/tam.ks
```

Note: The Administration API is available as a deprecated option for customers who were using it before the introduction of the Registry Direct API. All new deployments must use the Registry Direct API because the Administration API might not be available in subsequent IBM Security Access Manager releases. The Administration API is only needed in cases where the IBM Security Access Manager repository is not a standard LDAP server.

The `tam.conf` file that is generated in this step is used in a later configuration process.

For more information about configuring IBM Security Access Manager Runtime for Java, see Appendix A. com.tivoli.pd.jcfg.SvrSslCfg in *IBM Security Access Manager: Authorization Java Classes Developer Reference* and Appendix D. Registry Direct Java API ("Installation and configuration") in *IBM Security Access Manager: Administration Java Classes Developer Reference*.

Installing the IBM Security Access Manager Adapter utilities package

The IBM Security Access Manager Adapter utilities package contains Java classes that are used by the IBM Security Access Manager Adapter assembly lines.

Procedure

1. Copy `TAMComboUtils.jar` from the installation package to an appropriate IBM Tivoli Directory Integrator location:

   Windows

   ITDI_HOME\jars\connectors

   UNIX or Linux

   ITDI_HOME/jars/connectors

2. Restart the Dispatcher service if it is already installed and running.

   For information about starting and stopping the Dispatcher service, see the *Dispatcher Installation and Configuration Guide*.

Restarting the adapter service

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

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

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

Importing the adapter profile

An adapter profile defines the types of resources that the IBM Security Identity server can manage. It is packaged with the IBM Security Identity Adapter. Use the adapter profile to create an adapter service on IBM Security Identity server and establish communication with the adapter.

Before you begin

- The IBM Security Identity Governance and Intelligence server is installed and running.
- You have root or 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.The JAR file for the IBM Security Identity Governance and Intelligence is located in the `IGI-profile` folder of the installation package.

About this task

Target definition files are also called adapter profile files.

If the adapter profile is not installed correctly, the adapter cannot function correctly. You cannot create a service with the adapter profile or open an account on the service. You must import the adapter profile again.

Procedure

1. On the Appliance Dashboard, select Identity Governance and Intelligence Administration Console from the **Quick Links** widget. The Administration Console is displayed.
2. From the Administration Console, select **Target Administration**. The Target Administration console is displayed.
3. From the navigation tree, select **Manage Target Types**. The Manage Target Types page is displayed.
4. On the Manage Target Types page, click **Import**. The Import Target Type page is displayed.
5. On the Import Target Type page, complete these steps:

a. In the **Target Definition File** field, click **Browse** to locate the `<Adapter>Profile.jar` file. For example, if you are installing the IBM Security Identity Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
b. Click **OK**. A message indicates that you successfully imported a target type.

6. Click **Close**.

What to do next

- The import occurs asynchronously, which means it might take some time for the target type to load into the IBM Security Identity server from the properties files and to be available in other pages. On the Manage Target Types page, click **Refresh** to see the new target type. If the target type is not displayed in a reasonable amount of time, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. On the Appliance Dashboard, select **Manage System Settings** > **Maintenance** > **Log Retrieval and Configuration** > **Identity** > **trace log**, then click **View**.

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.

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 3. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Identity Governance and Intelligence.	"Adding a connector" on page 11.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 14.

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 SETUP Tab

Service name
Specify a name that defines this IBM Security Access Manager Adapter service on the IBM Security Identity server.

Note: Do not use slash signs "/" "\" in the service name. It is not allowed.

Description
Optionally, specify a description for this service.

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`.

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 4. 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 the service owner.

Service prerequisite
Optionally, specify the service prerequisite.

IBM SECURITY ACCESS MANAGER SETUP tab

IBM Security Access Manager API
The IBM Security Access Manager Adapter has two methods for managing IBM Security Access Manager user accounts and groups:

IBM Security Access Manager Administration API

This method is deprecated. It is only provided for use by customers whose IBM Security Access Manager server uses a non-standard LDAP repository.

IBM Security Access Manager Registry Direct API
This method uses the modern IBM Security Access Manager Registry Direct Java API. All deployments must use this method because it provides optimal performance and high availability support. For more information, see "Optimizing performance" on page 37.

Enable GSO Support
If checked, the adapter manages GSO-related account attributes and resource objects. When you manage GSO-related attributes and objects, the adapter uses the IBM Security Access Manager Administration API regardless of the value of the **IBM Security**

Access Manager API field in the service form. This is because the Registry Direct API does not support GSO management.

Use group cache on reconciliation
Enabling this option causes the IBM Security Access Manager Adapter to use an internal cache for resolving the group membership information for the users. In some circumstances, this option might improve the reconciliation performance. For more information, see "Optimizing performance" on page 37. Applies only when **IBM Security Access Manager Registry Direct API** is used.

Reload group cache on each reconciliation
Enabling this option causes the group cache to be reloaded on each reconciliation. For most cases, enable this option so the cache is up-to-date. In some circumstances, it might be useful to disable this option:

- Repeatedly running a full reconciliation for many users during testing.
- Environments in which the group membership information does not change or is irrelevant.

This option applies only when the **Use group cache on reconciliation** option is enabled.

Reconciliation Page Size
Optionally, apply only when you use IBM Security Access Manager Registry Direct API reconciliation.

If a page size other than 0 is specified, the IBM Security Access Manager Adapter uses **page mode** search to obtain user accounts information.

For more information, see "Reconciliation page size" on page 49.

IBM Security Access Manager Admin User
Specify the IBM Security Access Manager administrator account name (for example, `sec_master`). This account must have enough access rights to manage accounts.

IBM Security Access Manager Admin User Password
Specify the password for the IBM Security Access Manager administrator account.

IBM Security Access Manager Config File

Specify the file name and path for the configuration file that was created by using **SvrSslCfg** with the `–cfg_file` option during step "Configuring the IBM Tivoli Directory Integrator Java Runtime Environment into the IBM Security Access Manager secure domain" on page 8.

The example has this file path: `/opt/IBM/TDI/V7.1/timsol/tam.conf`.

Add Account
Specify the following options for adding IBM Security Access Manager user account:

Create user entry in registry.
Causes the adapter to create a user entry in the directory

server registry with a specific DN. If the entry exists, requests for account provisioning fail.

Import user entry from registry.
Causes the adapter to reuse an existing user entry from the directory server registry. If an entry with a specified DN does not exist, the request fails.

Import or create user entry.
Causes the adapter to check whether a user entry with a specific DN exists, and if so, this user entry is used. Otherwise, a new registry entry for the IBM Security Access Manager account is created.

Delete user entry from Registry
If this check box is checked, during the deletion of the IBM Security Access Manager account, the user entry is removed from the directory server registry. If the check box is left cleared, the user entry remains in the registry.

Add group
Specify one of the following options for adding IBM Security Access Manager groups:

Create group entry
Causes the adapter to create a group in the directory server registry with a specific DN. If the entry exists, the group cannot be created.

Import group entry
Causes the adapter to import an existing group entry from the directory server registry. Import fails when the entry with the DN specified does not exist.

Delete group entry from registry
If this check box is checked, during the deletion of the IBM Security Access Manager group, the group entry is removed from the directory server registry. If the check box is left cleared, the group entry remains in the registry.

Synchronize IBM Security Access Manager password in SSO Lockbox
If this check box is checked, during the password change operation, all of the account SSO credentials passwords are synchronized with the new account password.

IBM Security Access Manager Domain Name
Optionally, specify the IBM Security Access Manager Domain Name. If this field is left blank, the default IBM Security Access Manager runtime domain is used.

DISPATCHER ATTRIBUTES Tab

Disable AL Caching
Select the check box to disable the assembly line caching in the dispatcher for the service. The assembly lines for the add operation, modify operation, delete operation, and test operation 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 server.

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\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/profiles
```

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

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

Last status update: Date
Specifies the most recent date when the **Status and information** tab was updated.

Last status update: Time
Specifies the most recent time of the date when the **Status and information** tab was updated.

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

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

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

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

Dispatcher version
Specifies the version of the Dispatcher.

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

Adapter account
Specifies the account that running the adapter binary file.

Adapter up time: Date
Specifies the date when the adapter started.

Adapter up time: Time
Specifies the time of the date when the adapter started.

Adapter memory usage
Specifies the memory usage for running the adapter.

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

- Verify the adapter log to ensure that the test request was successfully sent to the adapter.
- Verify the adapter configuration information.
- Verify service parameters for the adapter profile. You might 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.

Upgrading the dispatcher

The new adapter package might require you to upgrade the Dispatcher.

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

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

The IBM Security Access Manager Adapter now supports the following dispatcher attributes:

- **Assembly Line File System Path**
- **Max Connection Count**
- **Disable Assembly Line Cache**

Upgrade your dispatcher to the latest version to support these new attributes.

Upgrading the adapter profile

The IBM Security Access Manager Adapter distribution package now contains only one main adapter profile: `itamprofile.jar`. It is a merge of the existing `itamprofile.jar` and `itamprofileAD.jar` files.

Use this profile when IBM Security Access Manager is configured against a supported LDAP server, Active Directory, Active Directory Application Mode (ADAM), or other supported user registries.

Note: For an IBM Security Identity Manager installation that uses Sun Directory Server, use `itamprofileSunDS.jar` to install the profile.

To import the profile, see "Importing the adapter profile" on page 10.

Chapter 5. Configuring

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

Configuring SSL authentication

To establish a secure connection between the adapter and the IBM Security Identity server, configure SSL authentication for connections that originate from the IBM Security Identity server or from the adapter. You can configure the adapter for one-way or two-way SSL authentication with signed certificates.

You must configure secure communication between IBM Security Identity server and IBM Security Access Manager Adapter.

Secure communication requires that SSL authentication is used between the various components.

You must configure secure communication between:

- IBM Security Identity server and IBM Security Access Manager Adapter. See "SSL configuration for IBM Security Identity server and IBM Security Access Manager Adapter"

  Note: When you configure Secure Sockets Layer (SSL) communication for the adapters that are based on IBM Tivoli Directory Integrator, you must configure SSL between WebSphere® Application Server and IBM Tivoli Directory Integrator.
- IBM Security Access Manager Adapter and Policy Server. See "Configuring the IBM Tivoli Directory Integrator Java Runtime Environment into the IBM Security Access Manager secure domain" on page 8

  Note: This communication path is used by the Access Manager Admin API. Even if the adapter is configured to use Registry Direct API, the Admin API is still needed to manage GSO credentials. This pathway is automatically setup for SSL via SvrSslCfg.
- IBM Security Access Manager Adapter and LDAP registry. See "Configuring Registry Direct API to use SSL" on page 26

  Note: The Registry Direct API bypasses the Policy Server and connects directly to the Access Manager LDAP repository. By default, this connection is unsecured, and additional steps are needed to configure it to use SSL.

SSL configuration for IBM Security Identity server and IBM Security Access Manager Adapter

When you configure Secure Sockets Layer (SSL) communication for the adapters that are based on IBM Tivoli Directory Integrator, you must configure SSL between WebSphere Application Server and IBM Tivoli Directory Integrator.

You must configure the IBM Tivoli Directory Integrator to use SSL. You must also configure WebSphere to use SSL by using the default keystore and default

truststore. For more WebSphere SSL configuration information, see the WebSphere online help available from the WebSphere Application Server Administrative Console.

For information about providing SSL communications between the IBM Security Identity server and the IBM Tivoli Directory Integrator server, see the *Dispatcher Installation and Configuration Guide*.

Configuring Registry Direct API to use SSL

To communicate securely with the Access Manager LDAP repository, you must configure the Registry Direct API to use SSL.

Procedure

1. Retrieve the Certificate Authority signer certificate chain that signed the certificate presented by the LDAP server. Usually there is only one signer certificate involved, but if there is a certificate chain, all signer certificates must be retrieved. Also, if multiple LDAP servers are involved, the signer certificates from all of them must be retrieved. Your LDAP administrator can provide this information.

   Note: When using the internal LDAP with the IBM Security Access Manager appliance, the certificate is self-signed. To retrieve the signer certificate, do the following procedures:

   a. Log in to the **Management Interface**.
   b. In **Secure Settings**. select **Manage System Settings** > **SSL Certificates**
   c. Select **embedded_ldap_keys**.
   d. In **Manage**, select **Edit SSL Certificate Database**.
   e. Select the **Personal Certificates** tab.
   f. Select the certificate name, **Server**.
   g. Select **Manage** > **Export**.
   h. Save the file in a temp directory.
2. In the Directory Integrator, `$SOLUTION_DIRECTORY`, open `solution.properties`.
3. Locate the configuration file for `javax.net.ssl.trustStore`.

   Note: This file must contain the signer certification for SSL to work.
4. Run `$ITDI_HOME/jvm/jre/bin/ikeyman`.
5. In `ikeyman`, open the `truststore` file that is defined in the `solution.properties`.

   Note:

   If you are using the default `serverapi/testadmin.jks` file, the password is 'administrator'.
6. Change the selection from **Personal Certificates** to **Signer Certificates**.
7. Click **Add**.
8. Select the certificate that you retrieved earlier and name it. For example, `ISAM LDAP`.

   Note: Repeat for any additional signer certificates in the chain.
9. Exit `ikeyman`.

10. In the Directory Integrator `$SOLUTION_DIRECTORY`, edit the `tam.conf` file that was created by SvrSslCfg. Ensure that the following two lines are set to 'true':
    - `ldap.ssl-enable=true`
    - `tls-v11-enable=true`
11. Restart the Directory Integrator Dispatcher process for the changes to take effect.

Customizing the adapter

You can use the configuration options to customize the IBM Security Access Manager Adapter.

The IBM Security Access Manager Adapter supports a standard set of attributes for default object classes that are used in IBM Security Access Manager servers. Because IBM Security Access Manager server requirements vary, you might customize or extend the IBM Security Access Manager Adapter schema to support more attributes or object classes.

Note: The adapter does not support modifying **UID**, **CN**, **principal name**, and attributes that form the Distinguished Name (DN).

Customizing the adapter profile

You can customize the adapter profile by enabling various user entry attributes for the default IBM Security Access Manager configurations.

User entry attributes for default IBM Security Access Manager configurations

The adapter profile by default enables on the account form only IBM Security Access Manager attributes.

The attribute labels, names, and types are listed in Table 5.

Table 5. Standard attributes supported by the IBM Security Access Manager Adapter

Name	Attribute name in schema	Schema	Note
User ID	eruid	Directory String	
User password	erpassword	Binary	
Password Last Changed	eritampwdlastchanged	Directory String	This attribute cannot be modified.
Distinguish Name	eritamdn	DN	
Full Name	cn	Directory String	
Last Name	sn	Directory String	
Description	description	Directory String	
Max number of failed logon	eritammaxfailedlogon	Integer	
Disable time interval	eritamdisabletime	Integer	
Max concurrent web sessions	eritameritammaxwebsessions	Integer	
Max password age	eritameritammaxpwdage	Integer	

Table 5. Standard attributes supported by the IBM Security Access Manager Adapter (continued)

Name	Attribute name in schema	Schema	Note
Do Not Enforce Password Policy	eritamppolicy	Boolean	
Change Password on Next Login	eritampvalid	Boolean	
Single Signon Capability	eritamsinglesign	Boolean	
Group Membership (multi-value attribute)	eritamgroupname	Directory String	
SSO Credentials (multi-value attribute)	eritamcred	Directory String	
Date of last access	erlastaccessdate	Directory String	
State of the account	eraccountstatus	Integer	

The IBM Security Access Manager Adapter is designed to work with user entry attributes from object classes that are defined in the IBM Security Access Manager configuration. Typically for non-Active Directory configuration, the user entry object classes are **inetOrgPerson**, **organizationPerson** and **Person**. For Active Directory typical configuration, the user entry object class is **User**.

The adapter schema contains attributes from **inetOrgPerson**, **organizationPerson**, and **Person** object classes. These attributes are shown in Table 6.

Table 6. The inetOrgPerson attributes supported by the IBM Security Access Manager Adapter

Attribute	Attribute	Attribute
BusinessCategory	homePostalAddress	PreferredLanguage
CarLicense	initials	RegisteredAddress
HomePhone	L	RoomNumber
DepartmentNumber	Mail	Secretary
preferreddeliverymethod	manager	UserPassword
DestinationIndicator	mobile	St
DisplayName	Pager	Street
EmployeeNumber	physicalDeliveryOfficeName	TelephoneNumber
EmployeeType	postalAddress	teletexTerminalIdentifier
FacsimileTelephoneNumber	postalCode	TelexNumber
GivenName	postOfficeBox	Title

The adapter schema also contains attributes from the **User** object class. Table 7 on page 29 lists attributes from the **User** object class only. Some of these attributes have different names in the IBM Security Identity server schema and Windows Active Directory schema. The names mapping and attribute description are also shown in this table.

Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter

Windows Active Directory Attribute	IBM Tivoli Directory Server Attribute	Description	Note
accountExpires	ntUserAcctExpires	Account expires on AD Account Tab	IBM Tivoli Directory Integrator does the advanced mapping to support this attribute.
c	c	Country/region on AD Address Tab	
co	co	Country/region on AD Address Tab	
company	company	Company on AD User Organization Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
countryCode	countryCode	Country/region on AD Address Tab	
department	department	Department on AD User Organization Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
displayName	displayName	Display name on AD General Tab	
facsimileTelephone Number	facsimileTelephone Number	Fax on AD Telephones Tab	
homeDirectory	NTUserHomeDir	Home folder: Local path/To on AD Profile Tab	IBM Tivoli Directory Integrator does the advanced mapping to support this attribute.
homeDrive	ntUserHomeDirDrive	Home folder: Connect on AD Profile Tab	IBM Tivoli Directory Integrator does the advanced mapping to support this attribute.
homePhone	homePhone	Home on AD Telephones Tab	
info	info	Notes® on AD Telephones Tab	
initials	initials	Initials on AD General Tab	

Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter (continued)

Windows Active Directory Attribute	IBM Tivoli Directory Server Attribute	Description	Note
ipPhone	ipPhone	IP phone on AD User Telephones Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
l	l	City on AD Address Tab	
mail	mail	Email on AD General Tab	
manager	manager	DN of manager on AD Organization Tab	
mobile	mobile		
otherFacsimile TelephoneNumber	otherFacsimile TelephoneNumber	Fax Number (Others) on AD User Telephones Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
otherHomePhone	otherHomePhone	Home Phone (Others) on AD User Telephones Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
otherIpPhone	otherIpPhone	IP Phone Number (Others) on AD User Telephones Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
otherMobile	otherMobile	Mobile Number (Others) on AD User Telephones Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.

Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter (continued)

Windows Active Directory Attribute	IBM Tivoli Directory Server Attribute	Description	Note
otherPager	otherPager	Pager Number (Others) on AD User Telephones Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
otherTelephone	otherTelephone	Phone Number (Others) on AD User General Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
pager	pager	Pager on AD Telephones Tab	
physicalDelivery OfficeName	physicalDelivery OfficeName	Office on AD General Tab	
postalCode	postalCode	Zip/Postal Code on AD Address Tab	
postOfficeBox	postOfficeBox	P.O. Box on AD Address Tab	
profilePath	profilePath	Profile path on AD User Profile Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
sAMAccountName	sAMAccountName	User logon name (preWindows 2000) on AD User Account Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.
scriptPath	ntUserScriptPath	Log on script on AD Profile Tab	IBM Tivoli Directory Integrator does the advanced mapping to support this attribute.
st	st	State/province on AD Address Tab	

Table 7. Mapping of Windows Active Directory User attributes supported by the IBM Security Access Manager Adapter (continued)

Windows Active Directory Attribute	IBM Tivoli Directory Server Attribute	Description	Note
streetAddress	streetAddress	Street on AD Address Tab	
telephoneNumber	telephoneNumber	Telephone number on AD General Tab	
title	title	Title on AD Organization Tab	
url	url	Web Page Address (Others) on AD General Tab	
userPrincipalName	userPrincipalName	User logon name on AD Account Tab	
userWorkstations	ntUserWorkstations	Log On To/Logon Workstations on AD Account Tab	IBM Tivoli Directory Integrator does the advanced mapping to support this attribute.
wWWHomePage	wWWHomePage	Web page on AD User General Tab	To support its management, this attribute is added to the IBM Tivoli Directory Server schema during the importation of the IBM Security Access Manager profile.

Attributes such as **userAccountControl**, non-modifiable attributes such as the **memberOf** and **logonHours** attribute are not supported. These attributes have INTEGER8 syntax; hence it would be difficult to manage them on the account form.

To manage any of the user entry attributes, complete the following steps:

1. Log in to the IBM Security Identity server as an Administrator.
2. Navigate to **Configuration** and then **Form Customization**.
3. Expand **Account** and then select the **itamaccount** Account.
4. Select the tab where you want to place an attribute.
5. From the attribute list, double-click the attribute to add it to the account form.
6. Click **Save Form Template**.

Adding attributes to Registry Direct reconciliation method

You can add IBM Security Access Manager attributes by modifying the `TamIterRgy` connector within the `TamSearch.xml` assembly line.

About this task

The Registry Direct reconciliation method is optimized to return a minimum set of attributes that are needed to manage an IBM Security Access Manager account. This method enhances performance by not retrieving sets of attributes that are not needed by most deployments. In some cases, however, there is a business need to

manage more IBM Security Access Manager account attributes from within IBM Security Identity server. This procedure allows those attributes to be reconciled by the adapter.

Procedure

1. Add an inetOrgPerson attribute or a custom object class attribute by using the Tivoli Directory Integrator 7.1 Configuration Editor. Do the following tasks:
   a. Open the `tamSearch.xml`**Assembly Line**.
   b. Select **TamIterRgy**.
   c. Click **Input Map**.
   d. Click **Add**.
   e. Enter the name of the new attribute. For example, mail.
   f. Click **OK**.
2. Save the assembly line changes.
3. Package the `itamprofile.jar` to include the modified `TamSearch.xml`.
4. Re-import the `itamprofile.jar` into the IBM Security Identity server.
5. Restart the RMI dispatcher.

Customizing the adapter workflows to provide credentials password in clear text

The adapter form for the attribute **`SSO Credentials`** creates a composite **`eritamcred`** attribute value that is sent to the adapter.

The attribute has this format:

```
<Resource Name> (Web Resource OR Group Resource)|
<Resource Account Name>|<Resource Password Base64 encoded>;
```

To specify initial resource password in a workflow, you must implement base64 encoding of the password.

The following example shows that a resource called `WebRsrc1`, of type `Web Resource`, with resource user ID `resid1` and resource password `pwd01` . The password `pwd01` has base64-encoding:

```
WebRsrc1 (Web Resource)|resid1|cHdkMDE=
```

The adapter offers alternative format for this attribute that makes it possible to specify the resource password in clear text, by putting prefix `{clear}`:

```
<Resource Name> (Web Resource OR Group Resource)|
<Resource Account Name>|{clear}<Resource Password in clear text>
```

This example of a web resource credential has a resource password that is set to "changeMe" concatenated with their surname:

```
WebRsrc1 (Web Resource)|resid1|{clear}changeMe" + subject.getProperty("sn")
```

Alternatively, you can still choose to assign a constant, simple, human-readable resource password. Here is an example of a group resource credential:

```
GroupRsrc2 (Group Resource)|resid2|{clear}tempPwd
```

Note:

- Resource passwords that are prefixed with `{clear}` must not contain the pipe character (`|`).

- There is no space between the string {clear} and password.
- If the string {clear} is incorrectly typed, the base64encode method that is used in the adapter does not report an error. A corrupted password is set.

Customizing the adapter to report corrupted or not well-formed accounts

The adapter user account attributes are the super set of IBM Security Access Manager user attributes and corresponding user registry attributes. During the reconciliation operation, the adapter merged those two sets of attributes into one.

About this task

If directory server is corrupted, some accounts can be corrupted to the point that only account name can be retrieved. By default the adapter is designed to log the error in the dispatcher log file and continue reconciliation.

The behavior can be changed to force reconciliation to stop on first corrupted account event.

Follow these steps to enable this feature:

Procedure

1. Extract the `itamprofile.jar` file by using the following command:

   ```
   jar -xvf itamprofile.jar
   ```

   Note: For an IBM Security Identity server installation that uses Sun Directory Server, use `itamprofileSunDS.jar`.
   Two directories are created:
   a. The directory `itamprofile` contains the adapter profile.
   b. The directory `META-INF` contains metadata for the JAR file.
2. Delete the `META-INF` directory. It is re-created by repackaging the adapter profile.
3. Under the `itamprofile` directory, in the `service.def`, change **`dispatcherParameter continueSearchOnMalformedAccount`** to `FALSE` for operation search. Use the following syntax:

   ```
   <dispatcherParameter name="continueSearchOnMalformedAccount">
   <default>FALSE</default>
   </dispatcherParameter>
   ```
4. Repackage the file by using the following command from a command prompt:

   ```
   jar -cvf itamprofile.jar itamprofile
   ```
5. Import the customized profile.
6. Restart the dispatcher.

What to do next

For more information about how to customize adapter profile, see the *IBM Security Identity server Custom Adapter Developer's Guide*.

Dispatcher configuration properties

Dispatcher configuration properties are set on the IBM Tivoli Directory Integrator.

For information about setting IBM Tivoli Directory Integrator configuration properties for the operation of the IBM Security Access Manager Adapter, see the *Dispatcher Installation and Configuration Guide*.

Using a custom IBM Security Access Manager object class

In some installations, a custom objectclass was added to IBM Security Access Manager accounts to provide more attributes to manage. The IBM Security Access Manager Adapter must be aware of these changes if IBM Security Identity server is managing them.

About this task

The method for specifying custom objectclasses was changed as of IBM Security Access Manager Adapter 6.0.20. All add and modify provisioning operations are now performed by using the Registry Direct API. As a result, custom objectclasses can no longer be specified on the IBM Security Access Manager service form.

Procedure

Include an extra parameter in the SvrSslCfg-generated `tam.conf` file that is used by Tivoli Directory Integrator to access IBM Security Access Manager.
The following parameter:
`ldap.user-objectclass=<yourobjectclass>;<yourobjectclass>;<yourobjectclass>`
The specified objectclasses are separated by semi-colons in the list.
For example:
`ldap.user-objectclass=customperson;inetorgperson;person`

Note: The **`ldap.user-objectclass`** is not a valid parameter when you use SvrSslCfg to generate the `tam.conf` file. Rather, it must be added manually to the `tam.conf` file after it is configured.

Related tasks:

"Adding attributes to Registry Direct reconciliation method" on page 32
You can add IBM Security Access Manager attributes by modifying the `TamIterRgy` connector within the `TamSearch.xml` assembly line.

Managing IBM Security Access Manager groups

You can manage IBM Security Access Manager groups by using the IBM Security Access Manager Adapter.

Add Group

You can add a group by either creating one or importing an existing group. The **Add Group** configuration option is available on the IBM Security Access Manager Service form.

The adapter creates new groups with the default object classes as specified by the IBM Security Access Manager Java Administration API. You cannot specify custom object classes when you use the adapter to create a group. However, you can use

the adapter to modify and delete IBM Security Access Manager groups with non-default object classes after they are imported.

When the adapter creates new groups it assigns them to the default group container, which is also specified by IBM Security Access Manager Java Administration API. By default, the adapter places new groups in the object space under `/Management/Groups`. You cannot specify a different group container when you use the adapter to create a group.

The parameters that are required on the IBM Security Identity Manager Add Group form are **group name** and **Distinguished Name (DN)**. You can also provide an optional **description**. The adapter does not support specifying a **Common Name(CN)** for the group, as the IBM Security Access Manager Java Administration API does not support this parameter. You cannot specify any other group attributes when you add a group.

Modify Group

You can use the IBM Security Access Manager Adapter to modify the group description.

The **`description`** attribute that is managed by the IBM Security Access Manager Java Administration API is the only group attribute that the adapter can modify. You cannot use the adapter to modify any other attributes present in the group registry entry. These attributes can include the **`UID`**, **`CN`**, **`principal name`**, and attributes that form the **`Distinguished Name`**.

Note: In Active Directory, an existing description cannot be modified to an empty string. This condition is a known limitation in the IBM Security Access Manager Java Administration API. The description remains unchanged if you attempt to modify it to an empty string.

Delete Group

You can use the adapter to delete IBM Security Access Manager groups.

If **Delete group entry from registry** is checked on the IBM Security Access Manager service form, then the entire group object is deleted from the registry. Otherwise, the group is removed from IBM Security Access Manager, but its registry object remains.

Group Operation Notes

Group operations are logged in the IBM Tivoli Directory Integrator `ibmdi.log` log file.

If a group operation is not successful, review the log for more detailed information.

Also, dynamic groups are not supported.

Enabling last login information

The adapter supports reconciling the last login information for determining dormant accounts.

About this task

To enable this feature, all IBM Security Access Manager servers must be configured to record the last login information. For more information about login information and dormant accounts, see the IBM Security Access Manager documentation.

Procedure

- In `webseald.conf`, ensure that the following parameter is set:

  ```
  enable-last-login = yes
  ```

- Configure the IBM Security Access Manager Policy Server to return the last login information. For example, in `ivmgrd.conf`, set the following parameter:

  ```
  provide-last-login = yes
  ```

Optimizing performance

Modifying the settings for the Dispatcher, the directory server, reconciliation, and group caching might improve the performance of the system.

Dispatcher tuning

You can modify the setting on the Dispatcher to optimize the performance.

For reconciling many entries, the following Dispatcher tuning settings are suggested for optimal performance:

- Edit `itim_listener.properties` in the IBM Tivoli Directory Integrator installation directory to set **`SearchResultSetSize`** to a larger value. For example, `SearchResultSetSize=1000`.

  This setting reduces the number of times that IBM Security Identity server must contact the adapter to fetch a subset of entries. Increasing this value causes IBM Security Identity server and the adapter to use more memory during reconciliation. You might also increase the JVM heap size for the Dispatcher and IBM Security Identity server.

- Increase the JVM heap size for Dispatcher. For example, on Windows edit the `ibmdiservice.props` file in the adapter `timsol` directory. Set the following property: `jvmcmdoptions=-Xms1024M –Xmx1024M`

  On UNIX systems, edit the IBM Tivoli Directory Integrator server start script. For example, `/opt/IBM/TDI/V7.1/ibmdirsrv`. Modify the Java command line:

  ```
  "$JRE_PATH/java" -Xms1024M -Xmx1024M -cp "/opt/IBM/TDI/V7.1/jars/3rdparty/
  IBM/db2jcc_license_c.jar" "-Dlog4j.configuration=file:etc/log4j.properties"
  -jar "/opt/IBM/TDI/V7.1/IDILoader.jar" com.ibm.di.server.RS "$@"
  ```

The Dispatcher must be restarted after these changes are made.

See the *Dispatcher Installation and Configuration Guide*.

Directory server performance tuning

Reconciliations retrieve a large amount of data from the IBM Security Access Manager user registry. The reconciliation performance of IBM Security Access Manager Adapter depends on the performance of the user registry.

To achieve the optimal performance, it is suggested that all documented performance tuning settings for the IBM Security Access Manager user registry be implemented.

For example, for IBM Tivoli Directory Server:

- Increase the **search result size limit** to be greater than the total number of entries that are required to be reconciled. For example, edit the `ibmslapd.conf` file to set the following parameter:

  ```
  ibm-slapdSizeLimit: 0
  ```

- Run **runstat** to help DB2® optimizer to determine the optimal accesses to the database.
- Run **reorgchk** and **reorg** to defragment the DB2 table spaces.
- Enable group members cache. If enough memory exists, set the maximum number of groups to the total number of groups. Set the maximum number of members to the number of members of the largest group. The first reconciliation is slower because it populates the cache.

The tests show that applying the preceding performance tuning settings improves the reconciliation performance especially for many users and groups with many members. This document does not describe all the performance tuning parameters for each user registry that is supported by IBM Security Access Manager. Review and configure all performance parameters to improve the general performance of the IBM Security Access Manager environment and any client that relies on it.

See these publications:

- *IBM Tivoli Directory Server: Performance Tuning and Capacity Planning Guide*
- *IBM Tivoli Directory Server: Administration Guide*
- *IBM Security Access Manager: Performance Tuning Guide*
- Vendor-specific documentation for other user registries that are supported by IBM Security Access Manager

Reconciliation method

Two reconciliation methods exist. Depending on your system, the method that you choose, might affect the performance during reconciliation.

Table 8. Reconciliation methods

IBM Security Access Manager API used	Menu selection
Administration API	IBM Security Access Manager Administration API
Registry Direct API	IBM Security Access Manager Registry Direct API

Use **Registry Direct API** when the IBM Security Access Manager user registry is an LDAP server. These factors improve performance:

- Use of the **ibm-allgroups** attribute for IBM Tivoli Directory Server.
- Direct access to the user registry instead of using the IBM Security Access Manager Policy Server.
- Use of multiple directory server replicas.

Group cache

Enabling the group cache for **Registry Direct API** reconciliation results in some performance improvement when there are many users and many small or empty groups.

When there are few groups or when the group cache is used within IBM Tivoli Directory Server, the benefit of using the adapter group cache is negligible. In addition, when there are groups with many members (for example, over 50000) using the group cache can negatively affect the reconciliation performance. The cache must be repopulated at the start of each reconciliation.

The group cache stores an internal representation of all users' group membership information. It requires a significant amount of memory. For 1 million users each belonging to 100 groups, approximately 1 GB of extra memory and JVM heap might be required for the adapter.

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?

Error messages and problem solving

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

Runtime Problems and corrective actions are described in the following table:

Table 9. Runtime Problems

Problem	Corrective Action

Reconciliation does not return all IBM Security Access Manager accounts. It returns 500 or 2048 accounts only.	The default settings for LDAP and IBM Security Access Manager have constraints on the search size limit. The best practice is as follows:
	1. Modify the IBM Tivoli Directory Server configuration file, `ibmslapd.conf`. This file is in the `etc` directory of the IBM Tivoli Directory Server. Set the **`ibm-slapdSizeLimit`** variable to 0 (no limit).
	2. Modify the IBM Security Access Manager LDAP `ldap.conf` configuration file in the `etc` directory of the IBM Security Access Manager Policy Server. Set the **`max-search-size`** variable to greater than 2048 (the default setting). Setting the **`max-search-size`** to 0 means that the search size is unlimited.
	3. Modify the IBM Security Access Manager configuration file, `pd.conf`, in the `etc` directory of the IBM Security Access Manager Policy Server. Set the **`ssl-v3-timeout`** variable to 84600 (the maximum setting) and set the **`ssl-io-inactivity`** variable to 0 (no limit).
	
	For ADAM only:
	
	Change the **`MaxResultSetSize`** and the **`MaxPageSize`** attribute to increase the search size limit on ADAM by using **`dsmgmt`**. The following example demonstrates setting the value of **`MaxResultSetSize`** and **`MaxPageSize`** to 200000 with the **ADAM Tools Command Prompt**:
	`C:\WINDOWS\ADAM>dsmgmt`
	`dsmgmt: LDAP Policies`
	`ldap policy: Connections`
	`server connections: Connect to server localhost:389`
	`Binding to localhost:389 ...`
	`Connected to localhost:389 using credentials`
	`of locally logged on user.`
	`server connections: Quit`
	`ldap policy: Show Values`
	`ldap policy: Set MaxResultSetSize to 200000`
	`ldap policy:Set MaxPageSize to 200000`
	`ldap policy:Commit Changes`
	
	For more information, see the ADAM Help.

Table 9. Runtime Problems (continued)

Problem	Corrective Action
Reconciliation does not return all IBM Security Access Manager accounts. Reconciliation is successful but some accounts are missing.	For the adapter to reconcile many accounts successfully, you can increase the WebSphere JVM memory. The following steps must be completed on the WebSphere host computer: **Note:** Do not increase the JVM memory to a value higher than the System memory. 1. Log in to the WebSphere Administrative Console. 2. Expand **Servers** in the left menu and select **Application Servers**. 3. A table displays the names of known application servers on your system. Click the link for your primary application server. 4. Select **Process Definition** from within the **Configuration** tab. 5. Select the **Java Virtual Machine** property. 6. Enter a new value for the **Maximum Heap Size**. The default value is 256 MB. The allocated JVM memory might not be large enough. In this case, an attempt to reconcile many accounts by using the IBM Security Access Manager adapter results in log file errors. The reconciliation process is not completed successfully. The adapter log files contain entries that state `ErmPduAddEntry failed`. The *`WebSphere_install_dir`*`/logs/itim.log` file contains `java.lang.OutOfMemoryError` exceptions.
The reconciliation of large numbers of IBM Security Access Manager accounts times out	During the reconciliation of large numbers of IBM Security Access Manager accounts (in the hundreds of thousands or millions), initialization of the reconciliation might take some time. This delay is hardware and performance-tuning dependent. Problems might occur as a result of timeout issues if you have IBM Tivoli Directory Server and DB2configured against your IBM Security Access Manager Policy Server. Refer to the IBM Tivoli Directory Server user guides for information about configuring the **`ibm-slapdIdleTimeOut`** value in the `ibmslapd.conf` file. As a guideline, this value can be increased to greater than 10,000 for the reconciliation of approximately 5 million accounts.

Table 9. Runtime Problems (continued)

Problem	Corrective Action
A search filter with an asterisk character returns more accounts that expected	A Search Filter can be specified for the IBM Security Access Manager reconciliation query. You can provide an LDAP filter in the Query page to specify a subset of accounts only (no supporting data) to be included in the reconciliation. Both the IBM Security Access Manager Administration API and Registry Direct API reconciliation methods support IBM Security Access Manager user account filtering. A subset of user accounts might be required. In this case, a Search Filter can be supplied that conforms to the IBM Security Access Manager pattern that was used to list User accounts. For example, a Search Filter to reconcile a subset of IBM Security Access Manager User accounts that include `JaneDoe`, `JonDoe` and `JimDolt` might be: `(eruid=J*Do*)`. The pattern for the **`eruid`** attribute is interpreted as a literal string. The asterisk (*) character, which is interpreted as a metacharacter that matches zero or more characters is the exception. Asterisks can be at the beginning, in the middle, or at the end of the pattern, and the pattern can contain multiple asterisks.
Enabling the option **Do not reconcile SSO credentials** removes all credentials IBM Security Identity registry.	Selecting this check box removes any current account credentials from IBM Security Identity registry after first successful reconciliation. The IBM Security Identity server considers any non-returned credential to mean that the credential no longer exists for the account. However, it is possible to retain any credentials that were reconciled previously by excluding the **`SSO credentials`** attribute from the reconciliation query.
The **Test** operation failed.	During a test of the IBM Security Access Manager service, the following message might be observed: `CTGIMT605E An error occurred while processing the CTGIMT401E An error occurred while starting the tamTest_TAMCombo on my_server-requestid_4329bac6-28ad-11b2-d8dc-00000930ab5b agent. Error: java.lang.NoClassDefFoundError: com/tivoli/pd/jutil/PDException operation on the IBM Tivoli Directory Integrator server. Error: {1}` This error might be because of either of the following reasons: • The IBM Tivoli Directory Integrator JVM is not configured with IBM Security Access Manager. • The Dispatcher was not stopped and restarted to pick up the change. Ensure that the IBM Security Access Manager Runtime for Java is installed and configured correctly. Alternatively, restart the Dispatcher as described in the *Dispatcher Installation and Configuration Guide*.

Table 9. Runtime Problems (continued)

Problem	Corrective Action
When you use the Registry Direct API, the first request after an extended time takes a long time to complete.	By default, the connection between the IBM Security Access Manager Registry Direct API and the LDAP servers is open indefinitely. If the connection is closed by a firewall, it might take 15-20 minutes for the API to detect this outage and open a new connection. In that situation, the following setting must be added to the `tam.conf` file used by the IBM Security Access Manager Adapter: `ldap.connection-inactivity = <value in seconds>` This setting must be set lower than the firewall stale connection timeout value. After you update the `tam.conf` file, restart the Directory Integrator process.

Reconciliation of supporting data

You can use search filters to limit the reconciliation of attributes such as **group names**.

The reconciliation of only **group names** is not currently supported. You can use a search filter to limit the attributes that are returned. For example:

`(eritamgroup=`*`pattern`*`)`

All supporting data can be reconciled by using the search filter in the reconciliation query. To reconcile supporting data only, the following search filter can be used:

`(!(objectclass=eritamaccount))`

Such a filter reconciles all non-account information.

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.

About this task

Uninstalling the adapter requires the removal of the JAR file and the removal of the adapter profile from IBM Security Identity server.

Note: The Dispatcher component must be installed on your system in order for adapters to function correctly in an IBM Tivoli Directory Integrator environment. If you delete the adapter profile for the IBM Security Access Manager Adapter, do not uninstall the Dispatcher.

Procedure

1. Stop the adapter service.
2. Remove the `TAMComboUtils.jar` file.
3. Start the adapter service.
4. Delete the IBM Security Access Manager profile from IBM Security Identity server.

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

Adapter attributes and object classes are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter. The IBM Security Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

For more information about IBM Security Access Manager Adapter attributes, see "User entry attributes for default IBM Security Access Manager configurations" on page 27.

Reconciliation page size

Page mode causes the directory server to return a specific number of entries in multiple chunks instead of all entries in a single chunk. The chunks are also called pages.

Not all directory servers support this option. Verify whether your directory server supports Page Mode before you use this option.

If your directory service supports Page Mode, use the **SearchResultSetSize** value of the Dispatcher **itim_listener.properties** file for this value.

To locate this value, see the *Dispatcher Installation and Configuration Guide*.

High availability support

Support for high availability is provided by the Access Manager Registry Direct API, which eliminates the dependency on the IBM Security Access Manager policy server.

You can configure the Registry Direct API against multiple directory servers for failover as well as load balancing. Due to limitations in Registry Direct API, high availability is not supported for:

- Active Directory and Domino user registries
- IBM Security Access Manager versions older than version 6.1 fix pack 6
- GSO management, including the lifecycle management of GSO enabled accounts

For more information about configuring Registry Direct API, see Appendix D that describes Registry Direct Java API installation and configuration in version 6.1.1 of the *IBM Tivoli Access Manager for e-business: Authorization Java Classes Developer Reference*.

Index

S

T

U

V

W

Printed in USA