IBM Security Identity Governance and Intelligence

SQL Server Adapter Installation and Configuration Guide

IBM Security Identity Governance and Intelligence

SQL Server 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.

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.

You can use the SQL Server Adapter to automate the following administrative tasks:

- Creating an account to authorize access to SQL server.
- Modifying an existing account to access SQL server.
- Removing access to a user account. This deletes the account from the SQL server.
- Suspending a user account by temporarily denying access to SQL server.
- Changing a user account password on SQL server.
- Reconciling user account information of all current accounts on SQL server.
- Reconciling the account information of a particular user account on SQL server by performing a lookup.

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 Adapter Development Kit based adapters, using `Setup.exe`

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

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 adapter binary.
2. Install 3rd party client libraries.
3. Set up the adapter environment.
4. Import the adapter profile.
5. Restart the adapter service.
6. Create an adapter service/target.
7. Install the adapter language package.
8. Verify that the adapter is working correctly.

Upgrade

You can do an upgrade or do a full installation. Review the *Release Notes* for the specific adapter before you proceed.

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. Uninstall the adapter binary
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. Prerequisites to install the adapter

Prerequisite	Description
Operating System	• Windows 2003 server Enterprise Edition 32-bit • Windows 2003 server Enterprise Edition 64-bit • Windows 2008 server 32-bit • Windows 2008 server 64-bit • Windows 2008 R2 server 32-bit • Windows 2008 R2 server 64-bit • Windows 7 32-bit • Windows 7 64-bit
Microsoft SQL Server	• MSSQL2012 The system where the adapter is installed must have SQL connectivity to the system where the SQL Server is installed.

Table 1. Prerequisites to install the adapter (continued)

Prerequisite	Description
Multiple Sites and Servers	A single SQL Server Adapter installation can be used by an organization with multiple MS SQL sites or multiple servers at an SQL site.
Network Connectivity	TCP/IP network.
System Administrator authority	To complete the adapter installation procedure, you must have system administrator authority.
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

Software downloads

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

Go to IBM Passport Advantage.

See the corresponding *IBM Security Identity server Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Installation worksheet

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

Table 2. Required information to install the adapter

Required information	Description
SQL Server client must be installed.	Before you install the SQL Server Adapter on its installation platform, install the SQL Server client software version 2012 on that system. For example, if you want to manage the SQL Server version 2012, the SQL Server client version 2012 must be installed on the system as the adapter.

Chapter 3. Installing

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

Installing the adapter

You can use these steps to install the adapter.

Before you begin

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

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

About this task

This task provides all the necessary steps for installing the SQL Server Adapter software.

Procedure

1. If you downloaded the installation software from Passport Advantage, perform the following steps:
   a. Create a temporary directory on the computer on which you want to install the software.
   b. Extract the contents of the compressed file into the temporary directory.
2. Start the installation program with the `setupwin32.exe` file in the temporary directory.
3. Click **Next** on the Welcome window.
4. Select either Full installation or Update installation and click Next to display the Select Destination Directory window. Remember that the adapter must already exist if you want to perform an updated installation.
5. Specify where you want to install the adapter in the Directory Name field. Do one of the following steps.
   - Click **Next** to accept the default location.
   - Click **Browse** and navigate to a different directory and click **Next**.
6. Review the installation settings in the Install Summary window and do one of the following steps:
   - Click **Back** and return to a previous window to change any of these settings.
   - Click **Next** when you are ready to begin the installation.
7. Click **Finish** when the software displays the Install Completed window.

Verifying the adapter installation

If the adapter is installed correctly, the following directories exist in the adapter installation directory.

bin The bin directory contains the following files:

- SqlServerAdapter.exe
- agentCfg.exe
- CertTool.exe
- fipsEnable.exe
- regis.exe
- IsamTool.exe

data Initially the data directory is empty.

log The log directory contains the adapter log file. After the adapter installation is complete and if the adapter service is *Started*, the adapter creates SqlServerAdapter.log file.

jre The jre directory contains the Java™ Standard Edition Runtime Environment. It provides complete runtime support for the Java applications.

_unist The _unist directory contains the uninstaller.exe and the DelRegKey.exe files. You can uninstall the SQL Server Adapter from the agent server workstation by using the uninstaller.exe file.

After the adapter installation completes, ensure that windows service for SQL Server Adapter is created and its status is *Started*. To view the windows service status:

1. Click **Start** > **Programs** > **Administrative Tools** > **Services** to display the Services page.
2. Search for the SQL Server Adapter service.

The adapter copies the following files to the system32 directory:

- AdkApi.dll
- ErmApi.dll
- ErmApiDaml.dll
- icudt36.dll
- icuuc36.dll
- libeay32.dll
- ssleay32.dll

Review the IBM_Security_Identity_Manager Sql_Server_Adapter_setInstallLog.log file in the adapter installation directory for any errors.

Restarting the adapter service

Perform the following steps to start and stop the SQL Server Adapter service.

Procedure

1. Click **Start** > **Programs** > **Administrative Tools** > **Services** to display the Services page.
2. Search for the SQL Server Adapter service
3. To start the service, right-click SQL Server Adapter and select **Start** from the pop-up menu.

4. To stop the service, right-click SQL Server Adapter and select **Stop** from the pop-up menu.

   Note: Do not stop the adapter service if the adapter is processing any requests.

Importing the adapter profile

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

Before you begin

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

About this task

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

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

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

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

Procedure

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

b. Click **Browse** to locate the JAR file that you want to import.
c. Click **Upload file**. A message indicates that you successfully imported a profile.

7. Click **Close**. The new profile is displayed in the list of profiles.

Results

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

What to do next

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

- Import the attribute mapping file. See "Importing attribute mapping file."
- Create a connector that uses the target profile. See "Adding a connector."

Importing attribute mapping file

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

About this task

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

Procedure

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

Adding a connector

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

Before you begin

Complete "Importing the adapter profile" on page 9.

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 10.
Ensure that you enabled the appropriate channel modes for the connector.	"Reviewing and setting channel modes for each new connector" on page 13.

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 12.

    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.

On the General Information tab:

Service Name
Specify a name that defines the adapter service on the IBM Security Identity server.

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

URL Specify the location and port number of the SQL Server Adapter. The port number is defined in the protocol configuration by using the `agentCfg` program.

User ID
Specify a Directory Access Markup Language (DAML) protocol user name. The user name is defined in the protocol configuration by using the `agentCfg` program.

Password
Specify the password for the DAML protocol user name. This password is defined in the protocol configuration by using the `agentCfg` program. For more information about the protocol configuration settings, see "Modifying protocol configuration settings" on page 25.

Owner
Optional: Specify the service owner, if any.

Service Prerequisite
Optional: Specify an existing service that is a prerequisite for the SQL server service.

SQL Server Name
Specify the instance name of SQL Server to be managed by this SQL Server Service. The instance name value is an IP address or host name.

Note: If `Always On` feature is enabled on your setup, then provide the Listener's VNN (Virtual Network Name) or Listener's IP address. Listener IP enables a client to connect to the current primary SQL instance.

SQL Admin Account
Specify the SQL Server instance administrator account name.

SQL Admin Password
Specify the SQL Server instance administrator account password.

Authentication
Specify an authentication mode by which the adapter connects to the SQL Server. From the dropdown menu , accept the default selection, **SQL Server Authentication**, or select **Windows Authentication**. With SQL Server authentication, the adapter uses the values from the **`SQL Admin Account`** and **`SQL Admin Password`** attributes for authentication.

With Windows authentication, the adapter uses the Windows account of the SQL Server Adapter windows service. The adapter uses the value from the **`Log On As`** attribute of the SQL Server Adapter Windows service. With Windows authentication, the adapter does not use the values from **`SQL Admin Account`** and **`SQL Admin Password`** attributes for authentication.

LocalSystem is the default Windows account of a SQL Server Adapter Windows service after the adapter installation. Change the Log On account to a domain Windows account that is also a member of the sysadmin Server role in the SQL Server instance to which the adapter is connecting. For example, `DOMAIN\user`.

Use SSL for Adapter to SQL Server Connection
Click this check box to use SSL communication between the adapter and the SQL Server. See your SQL Server product documentation to set up secure communication (SSL) between SQL Client and SQL Server. Only Windows authentication can be used with SSL. SSL Communication with SQL authentication is not supported.

Note: SSL is not supported by all versions of SQL Server. See your SQL Server product documentation before you configure the adapter to use SSL with the SQL Server.

On the Status and information tab

This 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.

ADK version
Specifies the version of the ADK that the adapter uses.

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

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

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

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

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

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

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

Verifying that the adapter is working correctly

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

Procedure

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

Chapter 4. Upgrading

You can upgrade either the SQL Server Adapter or the Adapter Development Kit (ADK).

Upgrading the adapter, as opposed to reinstalling it, allows you to keep your configuration settings. Additionally, you do not have to uninstall the current adapter and install the newer version.

Note: If your existing adapter version is earlier than 5.0, you must uninstall the older version of the adapter before you can install the 5.0 adapter. You cannot migrate from an earlier version to 5.0 because the encryption used in the 5.0 release is not compatible with previous ADK versions. Any previously encrypted values cannot be read by the 5.0 adapter.

The ADK is the base component of the adapter. While all adapters have the same ADK, the remaining adapter functionality is specific to the managed resource. You can perform an adapter upgrade to migrate your current adapter installation to a newer version, for example version 5.0 to version 5.*x*.

If only a code fix has been made to the ADK, instead of upgrading the entire adapter, you can upgrade just the ADK to the newer version. See "Upgrading the ADK" on page 20.

Upgrading the SQL Server Adapter

For adapter versions 5 and higher, use the adapter upgrade option:

About this task

- If you want to keep the adapter configuration (registry keys and certificates) unchanged.
- If the installed adapter is FIPS enabled. The Update Installation option keeps FIPS configurations such as the CA certificates, `fipsdata.txt` the (key generated by running `fipsenable.exe`) and the registry keys encrypted with fipsdata.txt unchanged.

If update installation option is selected, the path of the existing installed adapter is required. The installer replaces the binaries and the DLLs of the adapter and the ADK. The installer does not prompt for any configuration information during an update installation.

Note: Adapter related registry keys are not modified. The update installation does not create a new service for the adapter.

During an upgrade, in order to maintain all of your current configuration settings, as well as the certificate and private key, do not uninstall the old version of the adapter before installing the new version. During the install, specify the same installation directory where the previous adapter was installed.

In order to upgrade an existing adapter, complete the following steps:

Procedure

1. Stop the SQL Server Adapter service.
2. Install the new version of the adapter.

Results

When the upgraded adapter starts for the first time, new log files will be created, replacing the old files.

The adapter installer allows an update installation of the adapter, for adapters versions 5.0 or later.

Upgrading the ADK

You can use the ADK upgrade program to update the ADK portion of the adapters that are currently installed on a workstation.

About this task

This allows you to install just the ADK, and not the entire adapter. As part of the ADK upgrade, the ADK library and the DAML protocol library are updated. In addition, the **agentCfg** and certTool binaries are updated.

Note: Upgrading the ADK from versions 4.5 or 4.6 to 5.0 or a higher version is not supported.

The ADK consists of the runtime library, filtering and event notification functionality, protocol settings, and logging information. The remainder of the adapter is comprised of the Add, Modify, Delete, and Search functions. While all adapters have the same ADK, the remaining functionality is specific to the managed resource.

Before upgrading the ADK files, the upgrade program checks the current version of the ADK. A warning message occurs if the current level is higher than what you are attempting to install.

To upgrade the SQL Server Adapter ADK, complete the following steps:

Procedure

1. Download the ADK upgrade program compressed file from the IBM Web site.
2. Extract the contents of the compressed file into a temporary directory.
3. Stop the SQL Server Adapter service.
4. Start the upgrade program using the `adkinst_win32.exe` file in the temporary directory. For example, select **Run** from the **Start** menu, and type `C:\TEMP\adkinst_win32.exe` in the **Open** field.

   If no adapter is installed, you will receive the following error message, and the program exits:

   ```
   No Agent Installed - Cannot Install ADK.
   ```
5. In the Welcome window, click **Next**.
6. In the Software License Agreement window, review the license agreement and decide if you accept the terms of the license. If you do, click **Accept**.
7. On the Installation Information window, click **Next** to begin the installation.
8. On the Install Completed window, click **Finish** to exit the program.

Location of the ADK log files

Logging entries are stored in the *ADKVersion*`Installer.log` and *ADKVersion*`Installeropt.log` files, where *ADKVersion* is the version of the ADK. For example, `ADK50Installer.log` and `ADK50Installeropt.log`.

These files are created in the folder where you run the installation program.

Chapter 5. Configuring

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

Configuring the adapter

After you install the adapter, configure the adapter to function correctly.

About this task

Note: The screens in these tasks are examples. The actual screens might differ.

To configure the adapter, take the following steps:

Procedure

1. Start the adapter service. Use the Windows Services tool.
2. Configure the Directory Access Markup Language (DAML) protocol for the adapter to establish communication with the IBM Security Identity server.
3. Configure the adapter for event notification.
4. Install a certificate on the workstation where the adapter is installed and also on the IBM Security Identity server to establish secure communication between them.
5. Install the adapter profile on the IBM Security Identity server.
6. Configure the adapter service form.
7. Use the adapter configuration program, **agentCfg**, to view or modify the adapter parameters.
8. Configure the adapter account form.
9. Restart the adapter service after you modify the adapter configuration settings.

Starting the adapter configuration tool

Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

About this task

Note: The screens displayed in the tasks topics are examples. Information in the actual screens might be different.

Procedure

1. Browse to the Windows Command Prompt.
2. In the command prompt, change to the read/write `/bin` subdirectory of the adapter.If the adapter is installed in the default location for the read/write directory, run the following command.

   cd `C:\Program Files\IBM\ISIM\Agents\`*`adapter_name`*`\bin\`
3. Run the following command

   `agentCfg -agent` *`adapterAGNT`*
4. At the **Enter configuration key for Agent '*adapterAGNT*'**, type the configuration key for the adapter.

The default configuration key is `agent`.

Note: To prevent unauthorized access to the configuration of the adapter, you must modify the configuration key after the adapter installation completes..

The **Agent Main Configuration Menu** is displayed.

```
Agent Main Configuration Menu
-----------------------------------------
A. Configuration Settings.
B. Protocol Configuration.
C. Event Notification.
D. Change Configuration Key.
E. Activity Logging.
F. Registry Settings.
G. Advanced Settings.
H. Statistics.
I. Codepage Support.

X. Done.

Select menu option:
```

The following table lists the different options available in the **Agent Main Configuration Menu**.

Table 4. Options for the main configuration menu

Option	Configuration task
A	Viewing configuration settings
B	Changing protocol configuration settings
C	Configuring event notification
D	Changing the configuration key
E	Changing activity logging settings
F	Changing registry settings
G	Changing advanced settings
H	Viewing statistics
I	Changing code page settings

Viewing configuration settings

View the adapter configuration settings for information about the adapter, including version, ADK version, and adapter log file name.

Procedure

1. Access the **Agent Main Configuration** menu.
2. Type `A` to display the configuration settings for the adapter.

```
Configuration Settings
-----------------------------------------
Name            : adapter_nameAgent
Version         : 6.0.4.1200
ADK Version     : 6.0.1017
ERM Version     : 6.0.4.1200
Adapter Events  :
License         : NONE
Asynchronous ADD Requests  :  (Max.Threads:3)
Asynchronous MOD Requests  : (Max.Threads:3)
Asynchronous DEL Requests  :  (Max.Threads:3)
Asynchronous SEA Requests  :  (Max.Threads:3)
Available Protocols        : DAML
Configured Protocols       : DAML
Logging Enabled            : TRUE
Logging Directory          : C:\Program Files\IBM\ISIM\Agents\adapter_name\log
Log File Name              : adapter_name.log
Max. log files             : 3
Max.log file size (Mbytes) : 1
Debug Logging Enabled      : TRUE
Detail Logging Enabled     : FALSE
Thread Logging Enabled     : FALSE

Press any key to continue
```

3. Press any key to return to the **Main** menu.

Modifying protocol configuration settings

The adapter uses the DAML protocol to communicate with the IBM Security Identity server.

About this task

By default, when the adapter is installed, the DAML protocol is configured for a nonsecure environment. To configure a secure environment, use Secure Socket Layer (SSL) and install a certificate.

The DAML protocol is the only supported protocol that you can use. Do not add or remove a protocol.

Procedure

1. Access the Agent Main Configuration menu.
2. Type `B`. The DAML protocol is configured and available by default for the adapter.

```
Agent Protocol Configuration Menu
---------------------------------
Available Protocols: DAML
Configured Protocols: DAML
A. Add Protocol.
B. Remove Protocol.
C. Configure Protocol.

X. Done

Select menu option
```

3. At the Agent Protocol Configuration menu, type `C` to display the Configure Protocol Menu.

```
Configure Protocol Menu
-----------------------------------
A. DAML

X. Done

Select menu option:
```

4. Type a letter to display the Protocol Properties menu for the configured protocol with protocol properties.

   The following screen is an example of the DAML protocol properties.

```
DAML Protocol Properties
-------------------------------------------------------

A. USERNAME           ****** ;Authorized user name.
B. PASSWORD           ****** ;Authorized user password.
C. MAX_CONNECTIONS    100    ;Max Connections.
D. PORTNUMBER         45580  ;Protocol Server port number.
E. USE_SSL            FALSE  ;Use SSL secure connection.
F. SRV_NODENAME       _____  ;Event Notif. Server name.
G. SRV_PORTNUMBER     9443   ;Event Notif. Server port number.
H. HOSTADDR           ANY    ;Listen on address < or "ANY" >
I. VALIDATE_CLIENT_CE FALSE  ;Require client certificate.
J. REQUIRE_CERT_REG   FALSE  ;Require registered certificate.
K. READ_TIMEOUT       0      ;Socked read timeout (seconds)
X. Done
Select menu option:
```

5. Follow these steps to change a protocol value:
   - Type the letter of the menu option for the protocol property to configure. The following table describes each property.
   - Take one of the following actions:
     - Change the property value and press **Enter** to display the Protocol Properties menu with the new value.
     - If you do not want to change the value, press **Enter**.

Table 5. Options for the DAML protocol menu

Option	Configuration task
A	Displays the following prompt: `Modify Property 'USERNAME':` Type a user ID, for example, `agent`. The IBM Security Identity server uses this value to connect to the adapter. The default user ID is `agent`.
B	Displays the following prompt: `Modify Property 'PASSWORD':` Type a password, for example, `agent`. The IBM Security Identity server uses this value to connect to the adapter. The default password is `agent`.
C	Displays the following prompt: `Modify Property 'MAX_CONNECTIONS':` Enter the maximum number of concurrent open connections that the adapter supports. The default number is `100`.

Table 5. Options for the DAML protocol menu (continued)

Option	Configuration task
D	Displays the following prompt: `Modify Property 'PORTNUMBER':` Type a different port number. This value is the port number that the IBM Security Identity server uses to connect to the adapter. The default port number is `45580`.
E	Displays the following prompt: `Modify Property 'USE_SSL':` TRUE specifies to use a secure SSL connection to connect the adapter. If you set USE_SSL to TRUE, you must install a certificate. FALSE, the default value, specifies not to use a secure SSL connection. **Note:** By default event notification requires USE_SSL set to TRUE. To use event notification, you must set USE_SSL to TRUE and add a certificate and key from the PKCS12 file in the adapter.
F	Displays the following prompt: `Modify Property 'SRV_NODENAME':` Type a server name or an IP address of the workstation where you installed the IBM Security Identity server. This value is the DNS name or the IP address of the IBM Security Identity server that is used for event notification and asynchronous request processing. **Note:** If your operating system supports Internet Protocol version 6 (IPv6) connections, you can specify an IPv6 server.
G	Displays the following prompt: `Modify Property 'SRV_PORTNUMBER':` Type a different port number to access the IBM Security Identity server. The adapter uses this port number to connect to the IBM Security Identity server. The default port number is `9443`.
H	The HOSTADDR option is useful when the system where the adapter is running has more than one network adapter. You can select which IP address the adapter must listen to. The default value is `ANY`.

Table 5. Options for the DAML protocol menu (continued)

Option	Configuration task
I	Displays the following prompt: `Modify Property 'VALIDATE_CLIENT_CE':` Specify TRUE for the IBM Security Identity server to send a certificate when it communicates with the adapter. When you set this option to `TRUE`, you must configure options D through I. Specify FALSE, the default value to enable the IBM Security Identity server to communicate with the adapter without a certificate. **Note:** • The property name is VALIDATE_CLIENT_CERT; however, it is truncated by the `agentCfg` to fit in the screen. • You must use certTool to install the appropriate CA certificates and optionally register the IBM Security Identity server certificate.
J	Displays the following prompt: `Modify Property 'REQUIRE_CERT_REG':` This value applies when option I is set to `TRUE`. Type `TRUE` to register the adapter with the client certificate from the IBM Security Identity server before it accepts an SSL connection. Type `FALSE` to verify the client certificate against the list of CA certificates. The default value is `FALSE`.
K	Displays the following prompt: `Modify Property 'READ_TIMEOUT':` Type the timeout value in seconds for IBM Security Identity Governance and Intelligence and the adapter connection. This option applies to setups that have a firewall between IBM Security Identity Governance and Intelligence and the adapter. This firewall has a timeout value that is less than the maximum connection age DAML property on IBM Security Identity Governance and Intelligence. When your transactions run longer than the firewall timeout, the firewall terminates the connection. The sudden termination of connections might leave the adapter with incorrect connection threads causing the adapter to crash. When the adapter halts randomly because of the specified setup, change the value for the READ_TIMEOUT. The value must be in seconds and less than the timeout value of the firewall.

Table 5. Options for the DAML protocol menu (continued)

Option	Configuration task
L	Displays the following prompt: `Modify Property 'DISABLE_SSLV3':` SSLv3 is considered an unsecured protocol and is disabled by default. To enable SSLv3, set this value to FALSE. If this value does not exist or is not FALSE, the SSLv3 protocol will be disabled when using SSL. The DAML checks for an environment variable called *ISIM_ADAPTER_CIPHER_LIST*. This variable can contain a list of ciphers for the SSL protocol. DAML uses the openSSL library to support SSL. The cipher string is passed to openSSL during initialization. See the OpenSSL website at https://www.openssl.org/docs/apps/ciphers.html for the available cipher names and syntax. When this string is used, it only fails if none of the ciphers can be loaded. It is considered successful if at least one of the ciphers is loaded.

6. Follow these steps at the prompt:
   - Change the property value and press **Enter** to display the Protocol Properties menu with the new value.
   - If you do not want to change the value, press **Enter**.
7. Repeat step 5 to configure the other protocol properties.
8. At the Protocol Properties menu, type `X` to exit.

Related concepts:

"SSL certificate management with certTool" on page 50
Use the certTool utility to manage private keys and certificates.

"Configuring SSL authentication" on page 44
You can provide SSL authentication, certificates, and enable SSL authentication with the certTool utility.

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

"Installing the certificate" on page 53
After you receive your certificate from your trusted CA, install it in the registry of the adapter.

Configuring event notification

When you enable event notification, the workstation on which the adapter is installed maintains a database of the reconciliation data.

About this task

The adapter updates the database with the changes that are requested by the IBM Security Identity server and remains synchronized with the server. You can specify an interval for the event notification process to compare the database to the data that currently exists on the managed resource. When the interval elapses, the adapter forwards the differences between the managed resource and the database to IBM Security Identity server and updates the local snapshot database.

To enable event notification, ensure that the adapter is deployed on the managed host and is communicating successfully with IBM Security Identity Governance and Intelligence. You must also configure the host name, port number, and login information for the server and SSL authentication.

Procedure

- To identify the server that uses the DAML protocol and to configure SSL authentication, take the following steps:
  1. Access the Agent Main Configuration menu.
  2. At the Agent Protocol Configuration menu, select **Configure Protocol**.
  3. Change the USE_SSL property to `TRUE`.
  4. Install a certificate by using the certTool.
  5. Type the letter of the menu option for the SRV_NODENAME property.
  6. Specify the IP address or server name that identifies the server and press **Enter** to display the Protocol Properties menu with new settings.
  7. Type the letter of the menu option for the SRV_PORTNUMBER property.
  8. Specify the port number that the adapter uses to connect to the server for event notification.
  9. Press **Enter** to display the Protocol Properties menu with new settings.

  The example menu describes all the options that are displayed when you enable event notification. If you disable event notification, none of the options are displayed.
- To set event notification for the IBM Security Identity server, take the following steps:
  1. Access the Agent Main Configuration menu.
  2. At the Agent Main Configuration menu, type `C` to display the Event Notification menu.

```
Event Notification Menu
-----------------------------------------------------------------
* Password attributes       : eradapterPassword
* Reconciliation interval   : 1 hour(s)
* Next Reconciliation time  : 57 min(s). 36 sec(s).
* Configured Contexts       : subtest, outtest, tradewinds
A. Enabled - ADK
B. Time interval between reconciliations.
C. Set Processing cache size. (currently: 50 Mbytes)
D. Start event notification now.
E. Set attributes to be reconciled.
F. Reconciliation process priority.  (current: 1)
G. Add Event Notification Context.
H. Modify Event Notification Context.
I. Remove Event Notification Context.
J. List Event Notification Contexts.
K. Set password attribute names.

X. Done

Select menu option:
```

  3. At the Agent Main Configuration menu, type the letter of the menu option that you want to change.

     Note:

     – Enable option A for the values of the other options to take effect. Each time that you select this option, the state of the option changes.

– Press **Enter** to return to the Agent Event Notification menu without changing the value.

Table 6. Options for the event notification menu

Option	Configuration task
A	If you select this option, the adapter updates the IBM Security Identity server with changes to the adapter at regular intervals. If Enabled - Adapter is selected, the adapter code processes event notification by monitoring a change log on the managed resource. When the option is set to: • Disabled, all options except Start event notification now and Set attributes to be reconciled are available. Pressing the A key changes the setting to Enabled - ADK. • Enabled - ADK, all options are available. Pressing the `A` key changes the setting to Disabled or if your adapter supports event notification, changes to Enabled - Adapter. • Enabled - Adapter, all options are available except: Time interval between reconciliations, Set processing cache size, Start event notification now, Reconciliation process priority, and Set attributes to be reconciled. Pressing the `A` key changes the setting to Disabled. Type `A` to toggle between the options.

B	Displays the following prompt:
	`Enter new interval ([ww:dd:hh:mm:ss])`
	
	Type a different reconciliation interval. You can type this interval:
	`[00:01:00:00:00]`
	
	This value is the interval to wait after the event notification completes before it is run again. The event notification process is resource intense, therefore, this value must not be set to run frequently. This option is not available if you select Enabled - Adapter.

C	Displays the following prompt: `Enter new cache size[50]:` Type a different value to change the processing cache size. This option is not available if you select Enabled - Adapter.
D	If you select this option, event notification starts. This option is not available if you select Disabled or Enabled - Adapter.
E	Displays the Event Notification Entry Types menu. This option is not available if you select Disabled or Enabled - Adapter.
F	Displays the following prompt: `Enter new thread priority [1-10]:` Type a different thread value to change the event notification process priority. Setting the thread priority to a lower value reduces the impact that the event notification process has on the performance of the adapter. A lower value might also cause event notification to take longer.
G	Displays the following prompt: `Enter new context name:` Type the new context name and press **Enter**. The new context is added.
H	Displays a menu that lists the available contexts.

Table 6. Options for the event notification menu (continued)

Option	Configuration task
I	Displays the Remove Context menu. This option displays the following prompt: `Delete context context1? [no]:` Press **Enter** to exit without deleting the context or type `Yes` and press **Enter** to delete the context.

J	Displays the Event Notification Contexts in the following format:
	`Context Name : Context1`
	`Target DN : erservicename=context1,o=IBM,ou=IBM,dc=com`
	`--- Attributes for search request ---`
	`{search attributes listed} ---`

K	When you select the Set password attribute names, you can set the names of the attributes that contain passwords. These values are not stored in the state database and changes are not sent as events. This option avoids the risk of sending a delete request for the old password in clear text when IBM Security Identity Governance and Intelligence changes a password. Changes from IBM Security Identity Governance and Intelligence are recorded in the local database for event notification. A subsequent event notification does not retrieve the password. It sends a delete request for the old password in clear text that is listed in the IBM Security Identity Governance and Intelligence logs.

4. If you changed the value for options B, C, E, or F, press **Enter**. The other options are automatically changed when you type the corresponding letter of the menu option.

   The Event Notification menu is displayed with your new settings.

Related concepts:

"SSL certificate management with certTool" on page 50
Use the certTool utility to manage private keys and certificates.

Related tasks:

"Modifying protocol configuration settings" on page 25
The adapter uses the DAML protocol to communicate with the IBM Security Identity server.

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Setting event notification triggers

By default, all the attributes are queried for value changes.

About this task

Attributes that change frequently, for example, Password age or Last successful logon, must be omitted.

Note: Attributes for your adapter might be different than the attributes used in these examples.

Procedure

1. Access the **Agent Main Configuration** menu.
2. At the **Event Notification** menu, type `E` to display the **Event Notification Entry Types** menu.

```
Event Notification Entry Types
------------------------------------------
A. erAceServerAccount
B. erAceServerGroups
C. erAceServerClients
D. erAceServerTokens
E. erAceProfiles
X. Done
Select menu option:
```

Your adapter types might be different from this example. The types are not displayed in the menu until the following conditions are met:

a. Enable event notification
b. Create and configure a context
c. Perform a full reconciliation operation

3. Type `A` for a list of the attributes that are returned during a user reconciliation. Type `B` for attributes that are returned during a group reconciliation. Type `C` for a list of the attributes that are returned during client reconciliation. Type `D` for a list of the attributes that are returned during tokens reconciliation. Type `E` for a list of the attributes that are returned during profiles reconciliation.

   The **Event Notification Attribute Listing** for the selected type is displayed. The default setting lists all attributes that the adapter supports. The following list is an example of attributes that might be different for other adapters.

```
Event Notification Attribute Listing
------------------------------------
(a) **erAceGroupName     (b) **erAceToken3ActivatedDate      (c) **erAceTokenAssign
(d) **erAceToken2Assign  (e) **erAceToken2EnableDisableDate  (f) **erAceClearPin
(g) **erAceClearPin2     (h) **erAceClearPin3                (i) **erAceClient
(j) **erAceCreatePin     (k) **erAceToken1ActivatedDate      (l) **erAceDays
(m) **erAceTokenName     (o) **erAcePasswdActivatedDate      (p) **erAceDuration
(q) **erAceToken3Assign  (r) **erAceToken3EnableDisableDate  (s) **erAceTokenEnable

(p)rev    page 1 of 3  (n)ext
----------------------------

X. Done
Select menu option:
```

4. To exclude an attribute from an event notification, type the letter of the menu option.

   Note: Attributes that are marked with two asterisks (**) are returned during the event notification. Attributes that are not marked with ** are not returned during the event notification.

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Modifying an event notification context

Some adapters support multiple services.

About this task

An event notification context corresponds to a service on the IBM Security Identity server. If you want to enable event notification for a service, then you must create a context for the service. You can have multiple event notification contexts.

To modify an event notification context, do the following steps. In the following example screen, Context1, Context2, and Context3 are different contexts that have a different base point.

Procedure

1. Access the **Agent Main Configuration** menu.
2. From Event Notification, type the **Event Notification** menu option.
3. From the **Event Notification** menu, type the **Modify Event Notification Context** option to display a list of available contexts. For example:

```
Modify Context Menu
-------------------------------
A. Context1
B. Context2
C. Context3
X. Done
Select menu option:
```

4. Type the option of the context that you want to modify.

```
A. Set attributes for search
B. Target DN:
C. Delete Baseline Database
X. Done
Select menu option:
```

   Options:

Table 7. Options for modify context

Option	Configuration task
A	Adding search attributes for event notification
B	Configuring the target DN for event notification contexts
C	Removing the baseline database for event notification contexts

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Adding search attributes for event notification:

For some adapters, you can specify an attribute-value pair for one or more contexts.

About this task

These attribute-value pairs, which are defined by completing the following steps, serve multiple purposes:

- When a single adapter supports multiple services, each service must specify one or more attributes to differentiate the service from the other services.
- The adapter passes the search attributes to the event notification process either after the event notification interval occurs or the event notification starts manually. For each context, a complete search request is sent to the adapter. Additionally, the attributes that are specified for that context are passed to the adapter.

- When the IBM Security Identity server initiates a reconciliation process, the adapter replaces the local database that represents this service with the new database.

To add search attributes, do the following steps:

Procedure

1. Access the Agent Main Configuration menu.
2. At the Modify Context menu for the context, type `A` to display the Reconciliation Attribute Passed to Agent menu.

```
Reconciliation Attributes Passed to Agent for Context: Context1
------------------------------------------------------
A. Add new attribute
B. Modify attribute value
C. Remove attribute
X. Done
Select menu option:
```

   The adapter does not have any attributes that you must specify for Event Notification.

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Configuring the target DN for event notification contexts:

During event notification configuration, the adapter sends requests to a service that runs on the IBM Security Identity server.

About this task

You must configure target DN for event notification contexts for the adapter to know which service the adapter must send the request to. Configuring the target DN for event notification contexts involves specifying parameters, such as the adapter service name, organization (o), and organization name (ou).

Procedure

1. Access the Agent Main Configuration menu.
2. Type the option for Event Notification to display the Event Notification menu.
3. Type the option for Modify Event Notification Context, then enter the option of the context that you want to modify.
4. At the Modify Context menu for the context, type `B` to display the following prompt:

   ```
   Enter Target DN:
   ```

5. Type the target DN for the context and press **Enter**. The target DN for the event notification context must be in the following format:

   erservicename=*erservicename*,o=*organizationname*,ou=*tenantname*,rootsuffix

   Table 8 describes each DN element.

Table 8. DN elements and definitions

Element	Definition
erservicename	Specifies the name of the target service.

Table 8. DN elements and definitions (continued)

Element	Definition
o	Specifies the name of the organization.
ou	Specifies the name of the tenant under which the organization is. If this installation is an enterprise, then ou is the name of the organization.
rootsuffix	Specifies the root of the directory tree. This value is the same as the value of **Identity Manager DN Location** that is specified during the IBM Security Identity server installation.

Results

The Modify Context Menu displays the new target DN.

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Removing the baseline database for event notification contexts:

You can remove the baseline database for event notification contexts only after you create a context. You must also do a reconciliation operation on the context to create a Baseline Database file.

Procedure

1. From the **Agent Main Configuration** menu, type the **Event Notification** option.
2. From **Event Notification**, type the **Remove Event Notification Context** option to display the **Modify Context** menu.
3. Select the context that you want to remove.
4. Confirm that you want to remove a context and press **Enter** to remove the baseline database for event notification contexts.

Changing the configuration key

Use the configuration key as a password to access the configuration tool for the adapter.

Procedure

1. Access the **Agent Main Configuration Menu**.
2. At the **Main Menu** prompt, type `D`.
3. Do one of the following actions:
   - Change the value of the configuration key and press Enter. The default configuration key is **agent**. Ensure that your password is complex.
   - Press **Enter** to return to the **Main Configuration Menu** without changing the configuration key.

Results

The following message is displayed:

```
Configuration key is successfully changed.
```

The configuration program returns to the **Main Menu** prompt.

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Changing activity log settings

When you enable logging, the adapter maintains a log file of all transactions, *adapter_name*Agent.log.

About this task

By default, the log file is in the \log directory.

To change the adapter **activity logging** settings, take the following steps:

Procedure

1. Access the Agent Main Configuration menu.
2. At the **Main Menu** prompt, type E to display the Agent Activity Logging menu. The following screen displays the default **activity logging** settings.

```
Agent Activity Logging Menu
-----------------------------------
A. Activity Logging (Enabled).
B. Logging Directory (current: C:\Program Files\IBM\ISIM\Agents\adapter_nameAgent\log).
C. Activity Log File Name (current: adapter_nameAgent.log).
D. Activity Logging Max. File Size ( 1 mbytes)
E. Activity Logging Max. Files ( 3 )
F. Debug Logging (Enabled).
G. Detail Logging (Disabled).
H. Base Logging (Disabled).
I. Thread Logging (Disabled).
X. Done
Select menu option:
```

3. Perform one of the following steps:
   - Type the value for menu option B, C, D, or E and press **Enter**. The other options are changed automatically when you type the corresponding letter of the menu option. The following table describes each option.
   - Press **Enter** to return to the Agent Activity Logging menu without changing the value.

   Note: Ensure that Option A is enabled for the values of other options to take effect.

Table 9. Options for the **activity logging** *menu*

Option	Configuration task
A	Set this option to enabled to have the adapter maintain a dated log file of all transactions. When the option is set to: • Disabled, pressing the A to key changes to enabled. • Enabled, pressing the A to key changes to disabled. Type A to toggle between the options.

Table 9. Options for the **activity logging** *menu (continued)*

Option	Configuration task
B	Displays the following prompt: `Enter log file directory:` Type a different value for the logging directory, for example, `C:\Log`. When the logging option is enabled, details about each access request are stored in the logging file that is in this directory.
C	Displays the following prompt: `Enter log file name:` Type a different value for the log file name. When the logging option is enabled, details about each access request are stored in the logging file.
D	Displays the following prompt: `Enter maximum size of log files (mbytes):` Type a new value such as `10`. The oldest data is archived when the log file reaches the maximum file size. File size is measured in megabytes. It is possible for the activity log file size to exceed disk capacity.
E	Displays the following prompt: `Enter maximum number of log files to retain:` Type a new value up to 99 such as `5`. The adapter automatically deletes the oldest activity logs beyond the specified limit.
F	If this option is set to enabled, the adapter includes the debug statements in the log file of all transactions. When the option is set to: • Disabled, pressing the `F` key changes the value to enabled. • Enabled, pressing the `F` key changes the value to disabled. Type `F` to toggle between the options.
G	If this option is set to enabled, the adapter maintains a detailed log file of all transactions. The **detail logging** option must be used for diagnostic purposes only. Detailed logging enables more messages from the adapter and might increase the size of the logs. When the option is set to: • Disabled, pressing the `G` key changes the value to enabled. • Enabled, pressing the `G` key changes the value to disabled. Type `G` to toggle between the options.
H	If this option is set to enabled, the adapter maintains a log file of all transactions in the Adapter Development Kit (ADK) and library files. Base logging substantially increases the size of the logs. When the option is set to: • Disabled, pressing the `H` key changes the value to enabled. • Enabled, pressing the `H` key changes the value to disabled. Type `H` to toggle between the options.

Table 9. Options for the **activity logging** *menu (continued)*

Option	Configuration task
I	If this option is enabled, the log file contains thread IDs, in addition to a date and timestamp on every line of the file. When the option is set to: • Disabled, pressing the I key changes the value to enabled. • Enabled, pressing the I key changes the value to disabled. Type I to toggle between the options.

Modifying registry settings

Use the **Agent Registry Menu** to change the adapter registry settings.

Procedure

1. Type F (Registry Settings) at the main menu prompt to display the Registry menu:

```
adapter_name and version Agent Registry Menu
-----------------------------------------
A. Modify Non-encrypted registry settings.
B. Modify encrypted registry settings.
C. Multi-instance settings.
X. Done
Select menu option:
```

2. See the following procedures for modifying registry settings.

Modifying advanced settings

You can change the adapter thread count settings.

About this task

You can change the thread count settings for the following types of requests:

- System Login Add
- System Login Change
- System Login Delete
- Reconciliation

These settings determine the maximum number of requests that the adapter processes concurrently. To change these settings, take the following steps:

Procedure

1. Access the Agent Main Configuration menu.
2. At the **Main Menu** prompt, type G to display the Advanced Settings menu. The following screen displays the default thread count settings.

```
adapter_name and version number Advanced settings menu
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -

A. Single Thread Agent (current:FALSE)
B. ADD max. thread count. (current:3)
C. MODIFY max. thread count. (current:3)
D. DELETE max. thread count. (current:3)
E. SEARCH max. thread count. (current:3)
F. Allow User EXEC procedures (current:FALSE)
G. Archive Request Packets (current:FALSE)
H. UTF8 Conversion support (current:TRUE)
I. Pass search filter to agent (current:FALSE)
J. Thread Priority Level (1-10) (current:4)
X. Done
Select menu option:
```

Table 10. Options for advanced settings menu

Option	Description
A	Forces the adapter to allow only 1 request at a time. The default value is FALSE.
B	Limits the number of ADD requests that can run simultaneously. The default value is 3.
C	Limits the number of MODIFY requests that can run simultaneously. The default value is 3.
D	Limits the number of DELETE requests that can run simultaneously. The default value is 3.
E	Limits the number of SEARCH requests that can run simultaneously. The default value is 3.
F	Determines whether the adapter can do the pre-exec and post-exec functions. The default value is FALSE. **Note:** Enabling this option is a potential security risk.
G	This option is no longer supported.
H	This option is no longer supported.
I	Currently, this adapter does not support processing filters directly. This option must always be FALSE.
J	Sets the thread priority level for the adapter. The default value is 4.

3. Type the letter of the menu option that you want to change.
4. Change the value and press Enter to display the Advanced Settings menu with new settings.

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Viewing statistics

You can view an event log for the adapter.

Procedure

1. Access the **Agent Main Configuration Menu**.
2. At the **Main Menu** prompt, type `H` to display the activity history for the adapter.

```
  Agent Request Statistics
-----------------------------------------------------------------------
Date       Add       Mod       Del       Ssp       Res       Rec


-----------------------------------------------------------------

02/15/06  000001    000000    000000     000000    000000    000001

-----------------------------------------------------------------

X. Done
```

3. Type `X` to return to the **Main Configuration Menu**.

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Modifying code page settings

You can change the code page settings for the adapter.

About this task

To list the supported code page information for the adapter, the adapter must be running. Run the following command to view the code page information:

`agentCfg -agent [adapter_name] -codepages`

Procedure

1. Access the Agent Main Configuration menu.
2. At the **Main Menu** prompt, type `I` to display the Code Page Support menu.

```
adapter_name and version number Codepage Support Menu
-----------------------------------------
* Configured codepage: US-ASCII
-----------------------------------------
*
*****************************************
* Restart Agent After Configuring Codepages
*****************************************
A. Codepage Configure.
X. Done
Select menu option:
```

3. Type `A` to configure a code page.

   Note: The code page uses Unicode, therefore this option is not applicable.
4. Type `X` to return to the Main Configuration menu.

Related tasks:

"Starting the adapter configuration tool" on page 23
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

Accessing help and other options

Access the **agentCfg** help menu to view the list of available argument that you can use.

About this task

Note: The screens displayed in the tasks topics are examples. Information in the actual screens might be different.

Procedure

1. Access the **Agent Main Configuration Menu**.
2. Type `X` to display the command prompt.
3. Type **agentCfg** `-help` at the prompt to display the help menu and list of arguments.

```
Usage:
-version               ;Show version
-hostname <value>      ;Target nodename to connect to (Default:Local host IP address)
-findall               ;Find all agents on target node
-list                  ;List available agents on target node
-agent <value>         ;Name of agent
-tail                  ;Display agent's activity log
-portnumber <value>    ;Specified agent's TCP/IP port number
-netsearch <value>     ;Lookup agents hosted on specified subnet.
-codepages             ;Display list of available codepages.
-help                  ;Display this help screen
```

The following table describes each argument.

Table 11. Arguments and descriptions for the **agentCfg** *help menu*

Argument	Description
-version	Use this argument to display the version of the **agentCfg** tool.
-hostname *value*	Use the **-hostname** argument with one of the following arguments to specify a different host: • **-findall** • **-list** • **-tail** • **-agent** Enter a host name or IP address as the value.
-findall	Use this argument to search and display all port addresses 44970 - 44994 and their assigned adapter names. This option times out the unused port numbers, therefore, it might take several minutes to complete. Add the **-hostname** argument to search a remote host.

Table 11. Arguments and descriptions for the **agentCfg** *help menu (continued)*

Argument	Description
-list	Use this argument to display the adapters that are installed on the local host of the adapter. By default, the first time you install an adapter, it is either assigned to port address 44970 or to the next available port number. You can then assign all the later installed adapters to the next available port address. After the software finds an unused port, the listing stops. Use the **-hostname** argument to search a remote host.
-agent *value*	Use this argument to specify the adapter that you want to configure. Enter the adapter name as the value. Use this argument with the **-hostname** argument to modify the configuration setting from a remote host. You can also use this argument with the **-tail** argument.
-tail	Use this argument with the **-agent** argument to display the activity log for an adapter. Add the **-hostname** argument to display the log file for an adapter on a different host.
-portnumber *value*	Use this argument with the **-agent** argument to specify the port number that is used for connections for the **agentCfg** tool.
-netsearch *value*	Use this argument with the **-findall** argument to display all active adapters on the managed resource. You must specify a subnet address as the value.
-codepages	Use this argument to display a list of available code pages.
-help	Use this argument to display the Help information for the **agentCfg** command.

4. Type **agentCfg** before each argument that you want to run, as shown in the following examples.

   agentCfg -list

   Displays:

   - A list of all the adapters on the local host.
   - The IP address of the host.
   - The IP address of the local host.
   - The node on which the adapter is installed.

   The default node for the IBM Security Identity server must be 44970. The output is similar to the following example:

   ```
   Agent(s) installed on node '127.0.0.1'
   ----------------------
   adapterAGNT   (44970)
   ```

   agentCfg -agent ***adapterAGNT***

   Displays the main menu of the **agentCfg** tool, which you can use to view or modify the adapter parameters.

agentCfg -list -hostname 192.9.200.7

Displays a list of the adapters on a host with the IP address 192.9.200.7. Ensure that the default node for the adapter is 44970. The output is similar to the following example:

```
Agent(s) installed on node '192.9.200.7'
------------------
agentname   (44970)
```

agentCfg -agent *adapterAGNT* **-hostname 192.9.200.7**

Displays the **agentCfg** tool **Main menu** for a host with the IP address 192.9.200.7. Use the menu options to view or modify the adapter parameters.

Configuring SSL authentication

You can provide SSL authentication, certificates, and enable SSL authentication with the certTool utility.

For secure connection between the adapter and the server, configure the adapter and the server to use the Secure Sockets Layer (SSL) authentication with the DAML default communication protocol. Typically, SSL is used to establish a secure connection that encrypts the data that is being exchanged. While it can assist in authentication, you must enable registered certificates in DAML to use SSL for authentication. By configuring the adapter for SSL, the server can verify the identity of the adapter before the server makes a secure connection.

You can configure SSL authentication for connections that originate from the IBM Security Identity server or from the adapter. The IBM Security Identity server initiates a connection to the adapter to set or retrieve the value of a managed attribute on the adapter. Depending on the security requirements of your environment, you might configure SSL authentication for connections that originate from the adapter. For example, adapter events can notify the IBM Security Identity server of changes to attributes on the adapter. In this case, configure SSL authentication for web connections that originate from the adapter to the web server used by the IBM Security Identity server.

In a production environment, you must enable SSL security. If an external application communicates with the adapter (for example, the IBM Security Identity server) and uses server authentication, enable SSL on the adapter. Enabling SSL verifies the certificate that the application presents.

Running in SSL mode with Windows 2008

You can use Windows 2008 and run the adapter in Secure Socket Layer (SSL) mode.

About this task

Note: If you do not do these steps, the certificate is not installed completely and the SSL is not enabled. See http://en.wikipedia.org/wiki/User_Account_Control.

Procedure

1. Disable the User Account Control (UAC) security.
2. Install the required certificate.
3. (Optional) If required, enable the UAC security.

Related concepts:

"SSL certificate management with certTool" on page 50
Use the certTool utility to manage private keys and certificates.

Overview of SSL and digital certificates

In an enterprise network deployment, you must provide secure communication between the IBM Security Identity server and the software products and components with which the server communicates.

SSL protocol uses signed digital certificates from a certificate authority (CA) for authentication. SSL secures communication in a configuration. SSL provides encryption of the data that is exchanged between the applications. Encryption makes data that is transmitted over the network intelligible only to the intended recipient.

Signed digital certificates enable two applications that connect in a network to authenticate their identity. An application that acts as an SSL server presents its credentials to verify to an SSL client. The SSL client then verifies that the application is the entity it claims to be. You can configure an application that acts as an SSL server so that it requires the application that acts as an SSL client to present its credentials in a certificate. In this way, the two-way exchange of certificates is completed. A third-party certificate authority issues signed certificates for a fee. Some utilities, such as those provided by OpenSSL, can also provide signed certificates.

You must install a certificate authority certificate (CA certificate) to verify the origin of a signed digital certificate. When an application receives a signed certificate from another application, it uses a CA certificate to verify the certificate originator. A certificate authority can be:

- Well-known and widely used by other organizations.
- Local to a specific region or a company.

Many applications, such as web browsers, use the CA certificates of well-known certificate authorities. Using a well-known CA eliminates or reduces the task of distributing CA certificates throughout the security zones in a network.

Private keys, public keys, and digital certificates

Keys, digital certificates, and trusted certificate authorities establish and verify the identities of applications.

SSL uses public key encryption technology for authentication. In public key encryption, a public key and a private key are generated for an application. The data encrypted with the public key can be decrypted only with corresponding private key. Similarly, the data encrypted with the private key can be decrypted only by using the corresponding public key. The private key is password-protected in a key database file. Only the owner can access the private key to decrypt messages that are encrypted with the corresponding public key.

A signed digital certificate is an industry-standard method of verifying the authenticity of an entity, such as a server, a client, or an application. To ensure maximum security, a third-party certificate authority provides a certificate. A certificate contains the following information to verify the identity of an entity:

Organizational information
This certificate section contains information that uniquely identifies the

owner of the certificate, such as organizational name and address. You supply this information when you generate a certificate with a certificate management utility.

Public key
The receiver of the certificate uses the public key to decipher encrypted text that is sent by the certificate owner to verify its identity. A public key has a corresponding private key that encrypts the text.

Certificate authority's distinguished name
The issuer of the certificate identifies itself with this information.

Digital signature
The issuer of the certificate signs it with a digital signature to verify its authenticity. The corresponding CA certificate compares the signature to verify that the certificate is originated from a trusted certificate authority.

Web browsers, servers, and other SSL-enabled applications accept as genuine any digital certificate that is signed by a trusted certificate authority and is otherwise valid. For example, a digital certificate can be invalidated for the following reasons:

- The digital certificate expired.
- The CA certificate that is used to verify that it is expired.
- The distinguished name in the digital certificate of the server does not match with the distinguished name specified by the client.

Self-signed certificates

You can use self-signed certificates to test an SSL configuration before you create and install a signed certificate that is provided by a certificate authority.

A self-signed certificate contains a public key, information about the certificate owner, and the owner signature. It has an associated private key; however, it does not verify the origin of the certificate through a third-party certificate authority. After you generate a self-signed certificate on an SSL server application, you must:

1. Extract it.
2. Add it to the certificate registry of the SSL client application.

This procedure is equivalent to installing a CA certificate that corresponds to a server certificate. However, you do not include the private key in the file when you extract a self-signed certificate to use as the equivalent of a CA certificate.

Use a key management utility to:

- Generate a self-signed certificate.
- Generate a private key.
- Extract a self-signed certificate.
- Add a self-signed certificate.

Usage of self-signed certificates depends on your security requirements. To obtain the highest level of authentication between critical software components, do not use self-signed certificates or use them selectively. You can authenticate applications that protect server data with signed digital certificates. You can use self-signed certificates to authenticate web browsers or adapters.

If you are using self-signed certificates, you can substitute a self-signed certificate for a certificate and CA certificate pair.

Certificate and key formats

Certificates and keys are stored in the files with various formats.

.pem format

A privacy-enhanced mail (.pem) format file begins and ends with the following lines:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

A `.pem` file format supports multiple digital certificates, including a certificate chain. If your organization uses certificate chaining, use this format to create CA certificates.

.arm format

An `.arm` file contains a base-64 encoded ASCII representation of a certificate, including its public key, not a private key. The `.arm` file format is generated and used by the IBM Key Management utility.

.der format

A `.der` file contains binary data. You can use a`.der` file for a single certificate, unlike a `.pem` file, which can contain multiple certificates.

.pfx format (PKCS12)

A PKCS12 file is a portable file that contains a certificate and a corresponding private key. Use this format to convert from one type of SSL implementation to another. For example, you can create and export a PKCS12 file with the IBM Key Management utility. You can then import the file to another workstation with the certTool utility.

The use of SSL authentication

When you start the adapter, it loads the available connection protocols.

The DAML protocol is the only available protocol that supports SSL authentication. You can specify DAML SSL implementation.

The DAML SSL implementation uses a certificate registry to store private keys and certificates. The certTool key and certificate management tool manages the location of the certificate registry. You do not have to specify the location of the registry when you do certificate management tasks.

Configuring certificates for SSL authentication

You can configure the adapter for one-way or two-way SSL authentication with signed certificates.

About this task

Use the certTool utility for these tasks:

- "Configuring certificates for one-way SSL authentication"
- "Configuring certificates for two-way SSL authentication" on page 49
- "Configuring certificates when the adapter operates as an SSL client" on page 49

Configuring certificates for one-way SSL authentication

In this configuration, the IBM Security Identity server and the adapter use SSL.

About this task

Client authentication is not set on either application. The IBM Security Identity server operates as the SSL client and initiates the connection. The adapter operates as the SSL server and responds by sending its signed certificate to the IBM Security Identity server. The IBM Security Identity server uses the installed CA certificate to validate the certificate that is sent by the adapter.

In Figure 1, Application A operates as the IBM Security Identity server, and Application B operates as the adapter.

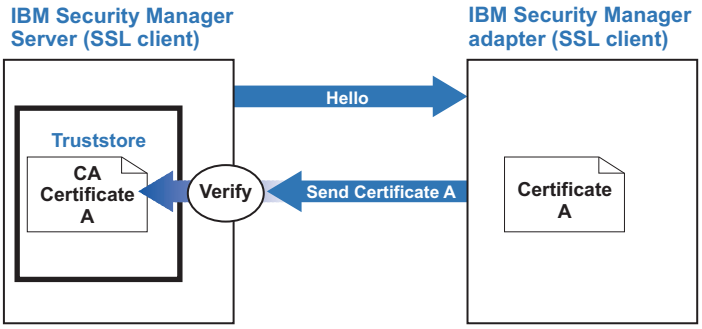

Figure 1. One-way SSL authentication (server authentication)

To configure one-way SSL, do the following tasks for each application:

Procedure

1. On the adapter, complete these steps:
   a. Start the certTool utility.
   b. To configure the SSL-server application with a signed certificate issued by a certificate authority:
      1) Create a certificate signing request (CSR) and private key. This step creates the certificate with an embedded public key and a separate private key and places the private key in the PENDING_KEY registry value.
      2) Submit the CSR to the certificate authority by using the instructions that are supplied by the CA. When you submit the CSR, specify that you want the root CA certificate to be returned with the server certificate.
2. On the IBM Security Identity server, do one of these steps:
   - If you used a signed certificate that is issued by a well-known CA:
     a. Ensure that the IBM Security Identity server stored the root certificate of the CA (CA certificate) in its truststore.
     b. If the truststore does not contain the CA certificate, extract the CA certificate from the adapter and add it to the truststore of the server.
   - If you generated the self-signed certificate on the IBM Security Identity server, the certificate is installed and requires no additional steps.
   - If you generated the self-signed certificate with the key management utility of another application:
     a. Extract the certificate from the keystore of that application.
     b. Add it to the truststore of the IBM Security Identity server.

Configuring certificates for two-way SSL authentication

In this configuration, the IBM Security Identity server and adapter use SSL.

About this task

The adapter uses client authentication. After the adapter sends its certificate to the server, the adapter requests identity verification from the IBM Security Identity server. The server sends its signed certificate to the adapter. Both applications are configured with signed certificates and corresponding CA certificates.

In the following figure, the IBM Security Identity server operates as Application A and the adapter operates as Application B.

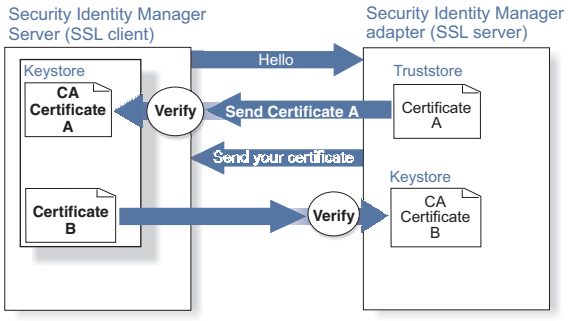

Figure 2. Two-way SSL authentication (client authentication)

Before you do the following procedure, configure the adapter and IBM Security Identity server for one-way SSL authentication. If you use signed certificates from a CA:

- The CA provides a configured adapter with a private key and a signed certificate.
- The signed certificate of the adapter provides the CA certification for the IBM Security Identity server.

To complete the certificate configuration for two-way SSL, do the following tasks:

Procedure

1. On the IBM Security Identity server, create a CSR and private key. Next, obtain a certificate from a CA, install the CA certificate, install the newly signed certificate, and extract the CA certificate to a temporary file.
2. On the adapter, add the CA certificate that was extracted from the keystore of the IBM Security Identity server to the adapter.

Results

After you configure the two-way certificate, each application has its own certificate and private key. Each application also has the certificate of the CA that issued the certificates.

"Configuring certificates for one-way SSL authentication" on page 47
In this configuration, the IBM Security Identity server and the adapter use SSL.

Configuring certificates when the adapter operates as an SSL client

In this configuration, the adapter operates as both an SSL client and as an SSL server.

About this task

This configuration applies if the adapter initiates a connection to the web server (used by the IBM Security Identity server) to send an event notification. For example, the adapter initiates the connection and the web server responds by presenting its certificate to the adapter.

Figure 3 describes how the adapter operates as an SSL server and an SSL client. To communicate with the IBM Security Identity server, the adapter sends its certificate for authentication. To communicate with the web server, the adapter receives the certificate of the web server.

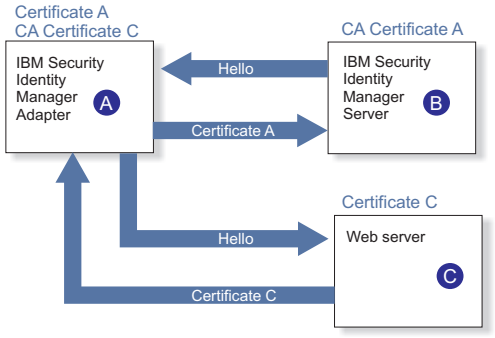

Figure 3. Adapter operating as an SSL server and an SSL client

If the web server is configured for two-way SSL authentication, it verifies the identity of the adapter. The adapter sends its signed certificate to the web server (not shown in the illustration). To enable two-way SSL authentication between the adapter and web server, take these steps:

Procedure

1. Configure the web server to use client authentication.
2. Follow the procedure for creating and installing a signed certificate on the web server.
3. Install the CA certificate on the adapter with the certTool utility.
4. Add the CA certificate corresponding to the signed certificate of the adapter to the web server.

What to do next

You can have the software send an event notification when the adapter initiates a connection to the web server (used by the IBM Security Identity server).

SSL certificate management with certTool

Use the certTool utility to manage private keys and certificates.

Starting certTool

To start the certificate configuration tool named certTool for the adapter, complete these steps:

Procedure

1. Click **Start** > **Programs** > **Accessories** > **Command Prompt**.

2. At a DOS command prompt, change to the `bin` directory for the adapter. If the directory is in the default location, type the following command:
   `cd C:\Program Files\IBM\ISIM\Agents\`*`adapter_name`*`\bin\`
3. Type `CertTool -agent` *`agent_name`* at the prompt.
   For example, to display the main menu, type: `CertTool -agent NotesAgent`

```
Main menu - Configuring agent: agentnameAgent
 ------------------------------
A. Generate private key and certificate request
B. Install certificate from file
C. Install certificate and key from PKCS12 file
D. View current installed certificate

E. List CA certificates
F. Install a CA certificate
G. Delete a CA certificate

H. List registered certificates
I. Register certificate
J. Unregister a certificate

K. Export certificate and key to PKCS12 file

X. Quit

Choice:
```

Results

From the **Main** menu, you can generate a private key and certificate request, install and delete certificates, register and unregister certificates, and list certificates. The following sections summarize the purpose of each group of options.

By using the first set of options (A through D), you can generate a CSR and install the returned signed certificate on the adapter.

A. Generate private key and certificate request
: Generate a CSR and the associated private key that is sent to the certificate authority.

B. Install certificate from file
: Install a certificate from a file. This file must be the signed certificate that is returned by the CA in response to the CSR that is generated by option A.

C. Install certificate and key from a PKCS12 file
: Install a certificate from a PKCS12 format file that includes both the public certificate and a private key. If options A and B are not used to obtain a certificate, the certificate that you use must be in PKCS12 format.

D. View current installed certificate
: View the certificate that is installed on the workstation where the adapter is installed.

With the second set of options, you can install root CA certificates on the adapter. A CA certificate validates the corresponding certificate that is presented by a client, such as the IBM Security Identity server.

E. List CA certificates
: Show the installed CA certificates. The adapter communicates only with IBM Security Identity server whose certificates are validated by one of the installed CA certificates.

F. Install a CA certificate
Install a new CA certificate so that certificates generated by this CA can be validated. The CA certificate file can either be in X.509 or PEM encoded formats.

G. Delete a CA certificate
Remove one of the installed CA certificates.

Options H through K apply to adapters that must authenticate the application to which the adapter is sending information. An example of an application is the IBM Security Identity server or the web server. Use these options to register certificates on the adapter.

If you configure the adapter for event notification or enable client authentication in DAML, you must install the CA certificate. The CA certificate must correspond to the signed certificate of the IBM Security Identity server. Use option F, **Install a CA certificate**.

H. List registered certificates
List all registered certificates that are accepted for communication.

I. Register a certificate
Register a new certificate. The certificate for registration must be in Base 64 encoded X.509 format or PEM.

J. Unregister a certificate
Unregister (remove) a certificate from the registered list.

K. Export certificate and key to PKCS12 file
Export a previously installed certificate and private key. You are prompted for the file name and a password for encryption.

Generating a private key and certificate request

A certificate signing request (CSR) is an unsigned certificate that is a text file.

About this task

When you submit an unsigned certificate to a certificate authority, the CA signs the certificate with the private digital signature. The signature is included in their corresponding CA certificate. When the CSR is signed, it becomes a valid certificate. A CSR contains information about your organization, such as the organization name, country, and the public key for your web server.

Procedure

1. At the **Main Menu** of the certTool, type `A`. The following message and prompt are displayed:
   ```
   Enter values for certificate request (press enter to skip value)
   ---------------------------------------------------------------------
   ```
2. At **Organization**, type your organization name and press **Enter**.
3. At **Organizational Unit**, type the organizational unit and press **Enter**.
4. At **Agent Name**, type the name of the adapter for which you are requesting a certificate and press **Enter**.
5. At **email**, type the email address of the contact person for this request and press **Enter**.
6. At **State**, type the state that the adapter is in and press **Enter**. For example, type `TX` if the adapter is in Texas. Some certificate authorities do not accept two letter abbreviations for states; type the full name of the state.

7. At **Country**, type the country that the adapter is in and press **Enter**.
8. At **Locality**, type the name of the city that the adapter is in and press **Enter**.
9. At **Accept these values**, take one of the following actions and press **Enter**:
   - Type `Y` to accept the displayed values.
   - Type `N` and specify different values.

   The private key and certificate request are generated after the values are accepted.
10. At **Enter name of file to store PEM cert request**, type the name of the file and press **Enter**. Specify the file that you want to use to store the values you specified in the previous steps.
11. Press **Enter** to continue. The certificate request and input values are written to the file that you specified. The file is copied to the adapter `bin` directory and the **Main** menu is displayed again.

Results

You can now request a certificate from a trusted CA by sending the `.pem` file that you generated to a certificate authority vendor.

Example of certificate signing request:

Here is an example certificate signing request (CSR) file.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB1jCCAT8CAQAwgZUxEjAQBgNVBAoTCWFjY2VzczM2MDEUMBIGA1UECxMLZW5n
aW5lZXJpbmcxEDAOBgNVBAMTB250YWdlbnQxJDAiBgkqhkiG9w0BCQEWFW50YWdl
bnRAYWNjZXNzMzYwLmNvbTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCkNhbGlmb3Ju
aWExDzANBgNVBAcTBklydmluZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
mR6AcPnwf6hLLc72BmUkAwaXcebtxCoCnnTH9uc8VuMHPbIMAgjuC4s91hPrilG7
UtlbOfy6X3R3kbeR8apRR9uLYrPIvQ1b4NK0whsytij6syCySaFQIB6V7RPBatFr
6XQ9hpsARdkGytZmGTgGTJ1hSS/jA6mbxpgmttz9HPECAwEAAaAAMA0GCSqGSIb3
DQEBAgUAA4GBADxA1cDkvXhgZntHkwT9tCTqUNV9sim8N/U15HgMRh177jVaHJqb
N1Er46vQSsOOOk4z2i/XwOmFkNNTXRVl9TLZZ/D+9mGZcDobcO+lbAKlePwyufxK
Xqdpu3d433H7xfJJSNYLYBFkrQJesITqKft0Q45gIjywIrbctVUCepL2
 -----END CERTIFICATE REQUEST-----
```

Installing the certificate

After you receive your certificate from your trusted CA, install it in the registry of the adapter.

Procedure

1. If you received the certificate as part of an email message, do the following actions.
   a. Copy the text of the certificate to a text file.
   b. Copy that file to the `bin` directory of the adapter.

   For Windows operating systems:

   `C:\Program Files\IBM\ISIM\Agents\`*`adapter_name`*`Agent\bin`
2. At the **Main Menu** prompt of the certTool, type `B`. The following prompt is displayed:

   ```
   Enter name of certificate file:
   --------------------------------------------------------------------------
   ```
3. At **Enter name of certificate file**, type the full path to the certificate file and press **Enter**.

   The certificate is installed in the registry for the adapter, and **Main Menu** is displayed again.

Installing the certificate and key from a PKCS12 file

If the certTool utility did not generate a CSR to obtain a certificate, you must install both the certificate and private key.

About this task

Store the certificate and private key in a PKCS12 file. The CA sends a PKCS12 file that has a `.pfx` extension. The file might be a password-protected file and it includes both the certificate and private key.

Procedure

1. Copy the PKCS12 file to the `bin` directory of the adapter.

   For Windows operating systems:

   `C:\Program Files\IBM\ISIM\Agents\`*`adapter_name`*`Agent\bin`
2. At the **Main Menu** prompt for the certTool, type `C` to display the following prompt:

   ```
   Enter name of PKCS12 file:
   --------------------------------------------------------------------------
   ```
3. At **Enter name of PKCS12 file**, type the name of the PKCS12 file that has the certificate and private key information and press **Enter**. For example, `DamlSrvr.pfx`.
4. At **Enter password**, type the password to access the file and press **Enter**.

Results

After you install the certificate and private key in the adapter registry, the certTool displays **Main Menu**.

View installed certificate

To list the certificate on your workstation, type `D` at the Main menu of certTool.

The utility displays the installed certificate and the Main menu. The following example shows an installed certificate:

```
The following certificate is currently installed.
Subject: c=US,st=California,l=Irvine,o=DAML,cn=DAML Server
```

Installing a CA certificate

If you use client authentication, you must install a CA certificate that is provided by a certificate authority vendor. You can install a CA certificate that was extracted in a temporary file.

Procedure

1. At the **Main Menu** prompt, type `F` (Install a CA certificate).

   The following prompt is displayed:

   ```
   Enter name of certificate file:
   ```
2. At **Enter name of certificate file**, type the name of the certificate file, such as `DamlCACerts.pem` and press **Enter**.

   The certificate file opens and the following prompt is displayed:

   ```
   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Install the CA? (Y/N)
   ```
3. At **Install the CA**, type `Y` to install the certificate and press **Enter**.

   The certificate file is installed in the `CACerts.pem` file.

Viewing CA certificates

Use the certTool utility to view a private key and certificate that are installed the adapter.

About this task

The certTool utility installs only one certificate and one private key.

Procedure

Type `E` at the **Main Menu** prompt.

Results

The certTool utility displays the installed CA certificates and the **Main** menu. The following example shows an installed CA certificate:

```
Subject: o=IBM,ou=SampleCACert,cn=TestCA
Valid To: Wed Jul 26 23:59:59 2006
```

Deleting a CA certificate

You can delete a CA certificate from the adapter directories.

Procedure

1. At the **Main Menu** prompt, type `G` to display a list of all CA certificates that are installed on the adapter.

   ```
   0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support
   Enter number of CA certificate to remove:
   ```

2. At **Enter number of CA certificate to remove**, type the number of the CA certificate that you want to remove and press **Enter**.

Results

After the CA certificate is deleted from the `CACerts.pem` file, the certTool displays the Main menu.

Viewing registered certificates

The adapter accepts only the requests that present a registered certificate when client validation is enabled.

Procedure

To view a list of all registered certificates, type `H` on the **Main Menu** prompt. The utility displays the registered certificates and the **Main** menu. The following example shows a list of the registered certificates:

```
0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support
```

Registering a certificate

You can register a certificate for the adapter.

Procedure

1. At the **Main Menu** prompt, type `I` to display the following prompt:

   ```
   Enter name of certificate file:
   ```

2. At **Enter name of certificate file**, type the name of the certificate file that you want to register and press **Enter**.

   The subject of the certificate is displayed, and a prompt is displayed, for example:

   ```
   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Register this CA? (Y/N)
   ```

3. At **Register this CA**, type `Y` to register the certificate, and press **Enter**.

Results

After you register the certificate to the adapter, the certTool displays the **Main** menu.

Unregistering a certificate

You can unregister a certificate for the adapter.

Procedure

1. At the **Main Menu**prompt, type `J` to display the registered certificates. The following example shows a list of lists registered certificates:

   ```
   0 - e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   1 - e=support@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Support,cn=Support
   ```

2. Type the number of the certificate file that you want to unregister and press **Enter**. For example:

   ```
   e=admin@ibm.com,c=US,st=California,l=Irvine,o=IBM,ou=Engineering,cn=Eng
   Unregister this CA? (Y/N)
   ```

3. At **Unregister this CA**, type `Y` to unregister the certificate and press **Enter**.

Results

After you remove the certificate from the list of registered certificate for the adapter, the certTool displays the **Main Menu**.

Exporting a certificate and key to a PKCS12 file

You can export a certificate and key to a PKCS12 file.

Procedure

1. At the **Main Menu** prompt, type `K` to display the following prompt:

   ```
   Enter name of PKCS12 file:
   ```

2. At the **Enter name of PKCS12 file** prompt, type the name of the PKCS12 file for the installed certificate or private key and press **Enter**.
3. At the **Enter Password** prompt, type the password for the PKCS12 file and press **Enter**.
4. At the **Confirm Password** prompt, type the password again and press **Enter**.

Results

After the certificate or private key is exported to the PKCS12 file, the certTool displays the Main menu.

Customizing the adapter

You can update the SQL Server Adapter JAR file, `SQL2000Profile.jar`, to change the adapter schema, account form, service form, and profile properties.

About this task

To make updates, extract the files from the JAR file, make changes to the necessary files, and repackage the JAR file with the updated files. Follow these steps in order to customize the SQL Server Adapter profile:

Procedure

1. Copy the JAR file to a temporary directory and extract the files. For more information on extracting the files, see "Copying the SQL2000Profile.jar file and extracting the files."
2. Make the appropriate file changes.
3. Install the new attributes on the IBM Security Identity Governance and Intelligence. For more information on updating this file, see "Creating a JAR file and installing new attributes on the IBM Security Identity Manager" on page 58.

Copying the SQL2000Profile.jar file and extracting the files

You can modify the profile JAR file to customize your environment.

About this task

The profile JAR file, SQL2000Profile.jar, is included in the SQL Server Adapter compressed file that you downloaded from the IBM Web site. The SQL2000Profile.jar file contains the following files:

- CustomLabels.properties
- erSQL2000Account.xml
- erSQL2000DAMLService.xml
- resource.def
- schema.dsml

When you finish updating the profile JAR file, install it on the IBM Security Identity Governance and Intelligence.

To modify the SQL2000Profile.jar file, complete the following steps:

Procedure

1. Log in to the system where the SQL Server Adapter is installed.
2. On the **Start** menu, click **Programs** > **Accessories** > **Command Prompt**.
3. Copy the SQL2000Profile.jar file into a temporary directory.
4. Extract the contents of` the SQL2000Profile.jar file into the temporary directory by running the following command:

   ```
   cd c:\temp
   jar -xvf SQL2000Profile.jar
   ```

   The jar command will create the c:\temp\SQL2000Profile directory.
5. Edit the appropriate file.

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 (For example, schema.dsml, CustomLabels.properties, and service.def).

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you see character ^*M* at the end of each line. This is the extra character 0x0d that is used to indicate a new line of text in MS-DOS. Tools, such as, `dos2unix` are used to remove the ^*M* character.

You might also want to use the text editors, such as, vi editor that ignore the ^*M* character. In the mentioned command, the ^*M* (or Ctrl-M) must be entered by pressing ^*v*^*M* (or Ctrl V Ctrl M) in sequence.

Example

For example, if you are using the vi editor, you can remove the ^*M* character by performing the following steps:

1. From the vi editor command mode, run the following command:

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

   and press **Enter**.

Enter the ^*M* (or Ctrl-M) by pressing ^*v*^*M* (or Ctrl V Ctrl M) in sequence. The ^*v* (or Ctrl V) preface indicates to the vi editor to use the next keystroke instead of considering the entry as a command.

Creating a JAR file and installing new attributes on the IBM Security Identity Manager

After you modify the `schema.dsml` and `CustomLabels.properties` files, you must import these files, and any other files that were modified for the adapter, into the IBM Security Identity Manager for the changes to take effect.

About this task

To install the new attributes, complete the following steps:

Procedure

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

   ```
   cd c:\temp
   jar -cvf SQL2000Profile.jar SQL2000Profile
   ```

2. Import the `SQL2000Profile.jar` file into the IBM Security Identity Manager Application Server.
3. Stop and start the IBM Security Identity Manager server.

What to do next

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not reflected immediately. Stop and start the IBM Security Identity Manager server to refresh the cache and the adapter schema.

Managing passwords during account restoration

When a person's accounts are restored from being previously suspended, you are prompted to supply a new password for the reinstated accounts. However, there are circumstances when you might want to circumvent this behavior.

About this task

The password requirement to restore an account on MS SQL falls into two categories: allowed and required. How each restore action interacts with its corresponding managed resource depends on either the managed resource, or the business processes that you implement. Certain resources will reject a password when a request is made to restore an account.

In this case, you can configure IBM Security Identity Governance and Intelligence to forego the new password requirement. If your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password, you can set the SQL Server Adapter to require a new password when the account is restored.

In the `resource.def` file, you can define whether a password is required as a new protocol option. When you import the adapter profile, if an option is not specified, the adapter profile importer determines the correct restoration password behavior.

Adapter profile components also enable remote services to find out if you discard a password that is entered by the user in a situation where multiple accounts on disparate resources are being restored. In this scenario, only some of the accounts being restored might require a password. Remote services will discard the password from the restore action for those managed resources that do not require them.

To configure the SQL Server Adapter to *not* prompt for a new password when restoring accounts:

Note: If you are upgrading an existing adapter profile, the new adapter profile schema will not be reflected immediately. You need to stop and start the IBM Security Identity server in order to refresh the cache and therefore the adapter schema.

Procedure

1. Stop the IBM Security Identity server.
2. Extract the files from the `SQL2000Profile.jar` file. For more information on customizing the adapter profile file, see "Customizing the adapter" on page 56.
3. Change to the `\SQL2000Profile` directory, where the `resource.def` file has been created.
4. Edit the `resource.def` file to add the new protocol options, for example:

   ```
   <Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
   PASSWORD_NOT_REQUIRED_ON_RESTORE" Value = "TRUE"/>
   <Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
   PASSWORD_NOT_ALLOWED_ON_RESTORE" Value = "FALSE"/>
   ```

   Adding the two options in the example above ensures that you will *not* be prompted for a password when an account is restored.
5. Create a new `SQL2000Profile.jar` file using the `resource.def` file and import the adapter profile file into the IBM Security Identity server.
6. Start the IBM Security Identity server again.

Verifying that the adapter is working correctly

After you install and configure the adapter, take steps to verify the installation.

Procedure

1. Test the connection for the service that you created on IBM Security Identity Governance and Intelligence.
2. Perform a full reconciliation from the IBM Security Identity server.
3. Perform all supported operations (add, change and delete) on one account and verify the `SqlServerAdapter.log` file after each operation to ensure that no errors were reported. For more information about the `SqlServerAdapter.log` file, see "Changing activity log settings" on page 37.

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

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

The following table contains warnings or errors which might be displayed in the user interface if the SQL Server Adapter is installed on your system.

Table 12. Warning and error messages

Warning or error message	Possible cause	Corrective action
Unable to establish connection with the SQL Server.	This error occurs when the managed resource is not up or when the value of following attributes are specified incorrectly on the service form: • Administrator name • Password	Ensure that the managed resource is up and the value of following attributes are specified correctly on the service form: • Administrator name • Password
LoginId already exists.	This error occurs when a request is made to add a user account that already exists.	Create a user account with another user ID.
LoginId does not exist on SQL server.	A request was made to either modify, suspend, restore, or delete a user account that does not exist on the managed resource.	Ensure that the user exists on the managed resource and is not directly deleted or modified on the managed resource.
Unsupported SQL Server Version.	This error when an attempt is made to manage the SQL Server that is not supported by the adapter.	Ensure that the SQL Server Adapter supports the SQL Server that you are using.
Fail to delete this account since "sa" is a system account.	This error occurs when an attempt is made to delete a system account sa.	The adapter returns the sa account in a reconciliation operation, however, you cannot delete this account. Do not manage this accounts from IBM Security Identity Governance and Intelligence.
Unable to add new loginId :: Microsoft OLE DB Provider for SQL Server :: Error #: 80040e14?The MUST_CHANGE option cannot be used when CHECK_EXPIRATION is OFF.	This error occurs when only the **User must change password** at next login check box is selected. Select the following check boxes on the Password tab of the account form and perform	Select the following check boxes on the Password tab of the account form and perform the operation again: • User must change password at next login • Enforce password expiration • Enforce password policy

Table 12. Warning and error messages (continued)

Warning or error message	Possible cause	Corrective action
Unable to add new loginId :: Microsoft OLE DB Provider for SQL Server :: Error #: 80040e14?The CHECK_EXPIRATION option cannot be used when CHECK_POLICY is OFF.	This error occurs when only the **Enforce password expiration** check box is selected.	Select the following check boxes on the Password tab of the account form and perform the operation again: • User must change password at next login • Enforce password expiration • Enforce password policy
Unable to add new loginId :: Microsoft OLE DB Provider for SQL Server :: Error #: 80040e14?Password validation failed. The password does not meet Windows policy requirements because it is too short.	This error occurs when: • The **Enforce password policy** check box is selected on the account form. • The value specified for the Password attribute on the account form does not meet the password policy requirements.	Check the: • Minimum password length • Password complexity • Password history requirements

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 the adapter involves running the uninstaller and removing the adapter profile from the IBM Security Identity server.

About this task

Before you remove the adapter, inform your users that the SQL Server Adapter is unavailable.

If the server is taken offline, adapter requests that were completed might not be recovered when the server is back online. To completely uninstall the SQL Server Adapter, perform these procedures:

Procedure

1. Uninstall the adapter from the target server.
2. Remove the adapter profile from the .

Uninstalling the adapter from the target server

You can remove the SQL Server Adapter.

Procedure

1. Stop the adapter service.
2. Run the uninstaller. To run the uninstaller:
   a. Navigate to the adapter home directory. For example, navigate to the `Tivoli/agents/`*`adaptername`*`/_uninst` directory.
   b. Double click the `uninstaller.exe` file.
   c. In the Welcome window, click **Next**.
   d. In the uninstallation summary window, click **Next**.
   e. Click **Finish**.
   f. Inspect the directory tree for the adapter directories, subdirectories, and files to verify that uninstall is complete.

Removing the adapter profile

Before you remove the adapter profile, ensure that no objects exist on your IBM Security Identity server that reference the adapter profile.

About this task

Examples of objects on the IBM Security Identity server that can reference the adapter profile are:

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

For specific information on how to remove the adapter profile, see the IBM Security Identity Governance and Intelligence product documentation.

Chapter 8. Reference

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

Adapter attributes and object classes

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.

Table 13. Attributes, descriptions, and data types

Attribute	Directory server attribute	Description	Data type
AccountPassword	erPassword	Specifies the password used to create a SQL Server account.	Binary
DatabaseRole	ersqldbrole	Specifies roles to be granted for the user mapped to the login ID in the database. If the user does not exist in the specified database then the adapter creates a user for the LoginId and grants specified database roles to that user. Specify the format on one line: `database_name: database_role_name` This role can be selected from the support data search box.	String
DatabaseUser	ersqldbuser	Specifies the user to which the LoginId is mapped in a database. Specify the format on one line: `database_name: user_name` A user with a login ID is created automatically in the login ID default database.	String
DefaultDatabase	erSQL2000DefDatabase	Specifies the default database for the user. If not provided, the default database is *master* with public as default permissions.	String
DefaultLanguage	erSQL2000DefLanguage	Specifies the default language of the user. If not provided, the form default is English.	String
LoginId	erUid	Specifies the login ID of the SQL Server or the Windows Mapped login in the SQL Server.	String

Table 13. Attributes, descriptions, and data types (continued)

Attribute	Directory server attribute	Description	Data type
ServerRole	erSQL2000ServerRole	Specifies the fixed server roles. Each roles has certain predefined permissions on the SQL Server. The roles can be granted and revoked from the SQL LoginId.	String

Adapter attributes by operations

Adapter attributes by operations refer to adapter actions by their functional transaction group. They are required for customization, creating provisioning rules, and understanding what service/target attributes are supported by the adapter.

System Login Add

A System Login Add is a request to create a user account with the specified attributes.

Table 14. Add request attributes

Required attribute	Optional attribute
erUid erSQL2000ServerName erSQL2000AdminAccount erServicePwd1	All other supported attributes

System Login Change

A System Login Change is a request to change one or more attributes for the specified users.

Table 15. Change request attributes

Required attribute	Optional attribute
erUid erSQL2000ServerName erSQL2000AdminAccount erServicePwd1	All other supported attributes

System Login Delete

A System Login Delete is a request to remove the specified user from the directory.

Table 16. Delete request attributes

Required attribute	Optional attribute
erUid erSQL2000ServerName erSQL2000AdminAccount erServicePwd1	None

System Login Suspend

A System Login Suspend is a request to disable a user account. The user is not removed and their attributes are not modified.

Table 17. Suspend request attributes

Required attribute	Optional attribute
erUid erAccountStatus erSQL2000ServerName erSQL2000AdminAccount erServicePwd1	None

System Login Restore

A System Login Restore is a request to activate a user account that was previously suspended. After an account is restored, the user can access the system with the same attributes as the ones before the Suspend function was called.

Table 18. Restore request attributes

Required attribute	Optional attribute
erUid erAccountStatus erSQL2000ServerName erSQL2000AdminAccount erServicePwd1	None

Reconciliation

The Reconciliation request synchronizes user account information between IBM Security Identity Governance and Intelligence and the adapter.

Table 19. Reconciliation request attributes

Required attribute	Optional attribute

Table 19. Reconciliation request attributes (continued)

erSQL2000ServerName erSQL2000AdminAccount erServicePwd1	None

Note:

- The adapter returns the BUILTIN\ADMINISTRATORS and sa accounts in a reconciliation operation, however, you cannot delete these accounts. Do not manage these accounts from SQL Server Adapter.
- The Database Access tab has the following attributes:
  - Database Role
  - Database User

The following table describes the syntax for specifying access and roles for the user on the Database Access tab on SQL Server Adapter:

Table 20. Syntax for specifying access and roles for the user on the Database Access tab

Attribute	**Syntax**	**Syntax**
Database Role	dbname:dbroleName	master:db_*owner*
Database User	dbname:dbuser	pubs:*user*

Special attributes

This topic is not applicable for this adapter.

Index

K

L

M

O

P

R

S

T

U

V

W

Printed in USA