IBM Security Verify Governance

Windows Local Account Adapter Installation and Configuration Guide

Contents

Figures

Tables

Chapter 1. Overview

An adapter is an interface between a managed resource and the Identity server. The Windows Local Account Adapter enables communication between the Identity server and the Windows 2008, and Windows 7 servers.

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

Features of the adapter

The Windows Local Account Adapter creates and manages local accounts on the Windows operating system.

The adapter runs in agent or agentless mode. You can install the adapter on a system other than the managed system. For information about running the adapter in agent or agentless mode, see "Installation worksheet" on page 7. Use the Windows Local Account Adapter to automate the following administrative tasks on Windows 2008, and Windows 7 servers:

- Create a user ID to authorize access to the Windows server.
- Modify an existing user ID to access the Windows server.
- Creating a home directory for a user ID.
- Remove access from a user ID. This deletes the user ID from the Windows server.
- Suspend a user account by temporarily deactivating access to the Windows server.
- Restore a user account by reactivating access to the Windows server.
- Change a user account password on the Windows server.
- Reconcile user information for all users on the Windows server.
- Reconcile user information for a specific user account on the Windows server.

The adapter also automates the following group management tasks:

- Reconcile group information for all the local groups on the Windows server.
- Creating local groups on the Windows server.
- Modifying group attributes.
- Removing groups from the Windows server.

Support Domain Accounts

After reconciliation, the adapter identifies all the domain users and group accounts in the local groups. The adapter also supports group management for domain members.

Domain users and groups can be added or deleted from the local group through IBM Security Verify Governance.

When adding domain users and groups, the user must specify the correct user name and group name. The adapter cannot perform the verification. The search widget is not provided.

Note:

- There must be a trust relationship between the domain and the machine on which the service runs.
- The user must specify the hostname in the service form **Workstation** field instead of giving the IPV6 address. Otherwise, the adapter cannot determine the hostname from the IPV6 address

Overview of SSL and digital certificates

In an enterprise network deployment, you must provide secure communication between the 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.

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.

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.

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 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
System	• A 32-bit x86-based microprocessor. • A minimum of 256 MB of memory. • At least 300 MB of free disk space.
Operating System	• Windows 7 • Windows Server 2008
Network Connectivity	Internet Protocol network
System Administrator Authority	The person who installs the Windows Local Account Adapter must have system administrator authority to complete the steps in this chapter.
Identity server	The following servers are supported: • Identity server Version 10.0 • Identity server Version 10.0 • IBM Security Privileged Identity Manager Version 2.0 • Identity server Version 10.0

Software downloads

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

Go to IBM Passport Advantage.

See the corresponding *IBM Security Verify Governance 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 on page 7 identifies the information you to install the adapter.

Table 2. Required information to install the adapter

Required information	Description
Administrator account on the managed resource for running the Windows Local Account Adapter in agent mode	An administrator account on the managed resource that has administrative rights. For example, you want to manage `Resource1` and the Windows Local Account Adapter is installed on `Resource1`, then `Admin1` account must be a member of administrator group on the managed resource `Resource1`. **Note:** Specify the name of the administrator account in the Windows Local Agent service on the Windows services page. The account must have appropriate privileges to administer the Windows Local Account users.

Table 2. Required information to install the adapter (continued)

Required information	Description
Administrator account on the managed resource for running the Windows Local Account Adapter in agentless mode	An administrator account on the managed resource that has administrative rights. For example, you are managing `Resource1` and the Windows Local Account Adapter is running on the `Resource2`. `Admin1` account must be a member of the administrator group on the managed resource `Resource1`. To run the adapter in agentless mode: • Enter the IP address or the machine name of `Resource1` on the service form. • Add a local account on the `Resource1` managed resource. The local account must be a member of the administrator group on the managed resource `Resource1`. **Note:** • Specify the name of the administrator account in the **Log On** tab of the Windows Local Agent service on the Windows services page. • When managing multiple resources with the Windows Local Account Adapter, the Administrator accounts must all have the same user name and password. The account information must match the information used for the **Log On** tab of the Adapter service. The accounts must be able to remotely connect to the Windows Local Account server and must have appropriate privileges to administer the Windows Local Account users.

Chapter 3. Installing in the Verify Governance virtual appliance

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

This procedure is applicable for a selected list of Identity Adapters. See the Identity Adapters product documentation to determine which adapters are supported in Identity Governance and Intelligence, and which can be installed on the virtual appliance.

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

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

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

   The adapter package includes the following files:

Table 3. Adapter package contents

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

Table 3. Adapter package contents (continued)	
Files	**Descriptions**
Additional adapter specific files	Examples of adapter specific files: • Connector jar files • Configuration files • Script files • Properties files The file names are specified in the adapter definition file along with the destination directory in the virtual appliance.

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

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

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

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

   c) Click **Open**.

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

   d) Click **OK**.

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

   b) Click **Edit**.

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

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

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

   c) Click the **Signer** tab.

   d) Click **Import**.

      The **Import Certificate** window is displayed.

   e) Browse for the certificate file.

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

   g) Click **Save**.

Chapter 4. Installing

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

Administrators can install the Windows Local Account Adapter software to provide an interface between a managed resource and the IBM Security Verify Governance Identity Manager server.

Installing the adapter binaries and libraries

Use this procedure to install the Windows Local Account Adapter software.

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

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

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 `setup.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 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 actions:
   - 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 actions:
   - 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

After the installation, you must verify that the necessary files and directories are created in the correct locations.

1. Verify that the following directories exist in the adapter installation directory:

   bin
   The `bin` directory contains the following files:
   - `WinLocalAgent.exe`
   - `agentCfg.exe`
   - `CertTool.exe`
   - `fipsEnable.exe`
   - `regis.exe`

   data
   Initially the `data` directory is empty.

license
The `license` directory contains files that provide license information in supported languages.

log
The `log` directory contains the adapter log files. After the adapter installation is complete, the adapter creates `WinLocalAgent.log` file.

_uninst
The `_uninst` directory contains the `uninstaller.exe` file. You can uninstall the Windows Local Account Adapter from the agent server workstation by using the `uninstaller.exe` file.

2. After the adapter installation completes, ensure that windows service for Windows Local Account Adapter is created and its status is *Started*.

   To view the windows service status:

   a. Click **Start** > **Programs** > **Administrative Tools** > **Services** to display the Services page.

   b. Search for the service for the Windows Local Account Adapter.

3. Ensure that the adapter copied the following files to the `system32` directory:

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

4. Review the installer log files (`WinLocalAdapter_Installer.log`) for any errors. The file is in the directory from where you run the adapter installation.

Restarting the adapter service

Various installation and configuration tasks might require the adapter to be restarted to apply the changes. You must restart the adapter if there are changes in the adapter profile or assembly lines. To restart the adapter, restart the adapter service.

Importing the adapter profile

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

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

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

The adapter profile definition file is used to create a target profile on the Verify Governance 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:

1. Log in to the Verify Governance 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.

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.

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

- Import the attribute mapping file. See “Importing attribute mapping file” on page 13.
- Create a connector that uses the target profile. See “Adding a connector” on page 14.

Importing attribute mapping file

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

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.

1. Log in to the Verify Governance 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 Verify Governance server, add a connector so that Verify Governance server can communicate with the managed resource.

Complete Importing the adapter profile.

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

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.

To add a connector, complete these steps.

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

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.

Enable the channel modes to synchronize the data between the target systems and Verify Governance. For more information, see “Enabling connectors” on page 15.

Enabling connectors

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

Table 4. Prerequisites for enabling a connector

Prerequisite	Find more information
A connector must exist in Verify Governance.	“Adding a connector” on page 14.
Ensure that you enabled the appropriate channel modes for the connector.	“Reviewing and setting channel modes for each new connector” on page 15.

To enable a connector, complete these steps:

1. Log in to the Verify Governance 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.

The connector is enabled

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

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.

Note: Legacy Verify Governance 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.

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

1. Log in to the Verify Governance 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 15.

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

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

Attribute Mapping

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

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

The file consists of Verify Governance 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.

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

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

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

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

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

Attribute	Mapped Attribute
eruid	CODE
erpassword	PASSWORD

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

Service/Target form details

Complete the service/target form fields.

On the General Information tab:

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

Description
Optional: Specify a description for this service.

URL
Specify the location and port number of the adapter. The port number is defined in the protocol configuration by using the **agentCfg** program. See "Modifying protocol configuration settings" on page 30.

If https is specified as part of the URL, the adapter must be configured to use SSL authentication. If the adapter is not configured to use SSL authentication, specify `http` for the URL. See "Configuring SSL authentication" on page 46.

User ID
Specify the DAML protocol user name. The user name is defined in the protocol configuration by using the **agentCfg** program. See "Modifying protocol configuration settings" on page 30.

Password
Specify the password for the DAML protocol user name. This password is defined in the protocol configuration by using the **agentCfg** program. See "Modifying protocol configuration settings" on page 30.

Work Station
Optional: Specify the location of the remote server that you want to manage. If this parameter is NULL, the adapter uses the local computer.

Owner
Optional: Specify the service owner, if any.

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

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

Verifying that the adapter is working correctly

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

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

Installing and uninstalling in silent mode

Silent mode suppresses the wizard and the Launcher User Interfaces (UIs) that do not display any information or require interaction.

You can use the **`-i silent`** option to install or uninstall the adapter in silent mode.

The adapter installer also installs run time libraries from Microsoft. The user interface of the installer for these run time libraries is also suppressed during silent installation of the adapter. The installer for these run time libraries creates a log file `vcredist_x86.log` in the `temp` directory of the *`user home`* directory. For example, `C:\Documents and Settings\Administrator\Local Settings\Temp\vcredist_x86.log`. Check this file for any errors.

Note:

- If you install the adapter in silent mode, the uninstaller runs in silent mode irrespective of whether you use the **`-i silent`** option or not.
- Silent uninstallation might not completely clean the installation directory. There might be some files or folders which are not removed. Check the installation folder and remove files and folder which are not required when the uninstallation is completed.

Adapter installation in silent mode

You can install the adapter in silent mode by using either command-line options or a response file.

Installing the adapter with default options

Run the following command from command line to install the Windows Local Account Adapter by using the –i silent option:

```
setup.exe –i silent -DLICENSE_ACCEPTED=TRUE
```

When you install the adapter by using the specified command, the adapter is installed with these default values.

Table 5. Default values	
Installation directory	%SYSTEM_DRIVE_ROOT%:\Program Files\IBM\ISIM\AgentsWinLocalAgent
Installation option	Full installation

Installing the adapter with command-line options

You can specify the listed installation options from the command line when you install the adapter by using the silent mode. For example, if you want to override the default installation directory path, run the following command:

```
setup.exe –i silent  -DLICENSE_ACCEPTED=TRUE
-DUSER_INSTALL_DIR="c:\security\MyFolder"
```

Note:

- The -D option is followed by a variable and a value pair without any space after the -D option.
- You must wrap arguments with quotation marks when the arguments contain spaces.

Table 6. Command-line options

Option	Description	Default value
DLICENSE_ACCEPTED	The installer uses this parameter to get the license acceptance state. When the value is TRUE, it indicates that you accept the terms in the license agreement of the adapter. If the value of this parameter is FALSE or if this parameter is missing then the installation stops. This parameter is required for silent installation.	FALSE
DUSER_INSTALL_DIR	Value overrides the default installation directory path. For example, -DUSER_INSTALL_DIR="D:\security\MyFolder". **Note:** The installation path must be wrapped in quotations marks.	%SYSTEM_DRIVE_ROOT%:\Program Files\IBM\ISIM\Agents\WinLocalAgent
DUSER_INPUT_INSTALL_TYPE_1	When the value of this parameter is \"Full Installation\" the installer performs full installation of the adapter. For example, DUSER_INPUT_INSTALL_TYPE_1=\"Full Installation\"	\"Full Installation\"
DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1	This parameter is associated with DUSER_INPUT_INSTALL_TYPE_1. When the value of this parameter is 1 the installer performs full installation of the adapter. You can either use **DUSER_INPUT_INSTALL_TYPE_1** or **DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1** or both to perform full installation.	1
DUSER_INPUT_INSTALL_TYPE_2	When the value of this parameter is \"Update Installation\", the installer performs update installation of the adapter. For example, DUSER_INPUT_INSTALL_TYPE_2=\"Update Installation\" **Note:** When \"Update Installation\" is specified as the value for this parameter, do not specify **DUSER_INPUT_INSTALL_TYPE_1**. If it is specified set the value to blank. You must also set value of **DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1** to 0.	No default value.

Table 6. Command-line options (continued)

Option	Description	Default value
`DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2`	This parameter is associated with **DUSER_INPUT_INSTALL_TYPE_2**. When the value of this parameter is 1 the installer performs update installation of the adapter. You can either use **DUSER_INPUT_INSTALL_TYPE_2** or **DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2** or both to perform update installation. **Note:** When the value 1 is specified for this parameter, do not specify **DUSER_INPUT_INSTALL_TYPE_1**. If it is specified set the value to blank. You must also set the value of **DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1** to `0`.	`0`

Installing the adapter by using the response file

Generating the response file

You can use response file to provide inputs during silent installation. Generate the response file by running the following command, which runs the installer in interactive mode and installs the adapter.

```
setup.exe –r "Full path of response file"
```

For example:

```
setup.exe –r "C:\Temp\WinLocalResponse.txt"
```

Note: If you run this command to generate only the response file, you must uninstall the adapter by using the uninstaller.

Creating the response file manually

You can also manually create the response file with the following content:

```
#Has the license been accepted
#-----------------------------
LICENSE_ACCEPTED=TRUE

#Select Install Type
#-------------------
USER_INPUT_INSTALL_TYPE=\"Full Installation\",\"\"
USER_INPUT_INSTALL_TYPE_1=Full Installation
USER_INPUT_INSTALL_TYPE_2=
USER_INPUT_INSTALL_TYPE_BOOLEAN_1=1
USER_INPUT_INSTALL_TYPE_BOOLEAN_2=0

#Choose Install Folder
#---------------------
USER_INSTALL_DIR=C:\\Program Files\\IBM\\ISIM\\Agents\\WinLocalAgent
```

After you create the response file, you can use it to provide parameters to the installer for silent installation.

```
setup.exe –i silent -f "Full path of response file"
```

For example:

```
setup.exe –i silent -f "C:\WinLocalInstallParameters.txt"
```

Adapter uninstallation in silent mode

Run the following command from the command line to uninstall the Windows Local Account Adapter by using the –i silent option.

Specify the full path when you are not running the command from the `_uninst` directory in the installation directory of the adapter.

```
uninstaller.exe -i silent
```

For example, `"C:\Program Files\IBM\ISIM\Agents\WinLocalAgent\_uninst\uninstaller.exe" -i silent`.

Note: Restart the workstation after you install or uninstall the adapter.

Chapter 5. Upgrading

You can either update the Windows Local Account Adapter or the Adapter Development Kit (ADK).

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.

Note: If your existing adapter version is earlier than 6.0, you must uninstall the older version of the adapter before you can install the 6.*x* adapter. Version earlier than 6.0 cannot be updated to a 6.*x* ADK.

You can perform an adapter upgrade to migrate your current adapter installation to a newer version, for example version 6.0 to version 6.*x*. Upgrading the adapter, as opposed to reinstalling it, enables you to keep your configuration settings. Additionally, you do not have to uninstall the current adapter and install the newer version.

If you make a code fix only 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 25.

Upgrading the Windows Local Account Adapter

You can update the Windows Local Account Adapter.

For adapter versions 6.0 and later, use the adapter update option:

- 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 unchanged. For example, the CA certificates, `fipsdata.txt` (the key generated by running `fipsenable.exe`), and the registry keys encrypted with `fipsdata.txt` are unchanged.

If the update installation option is selected, the path of the existing installed adapter is required. The installer replaces the binary files 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 service for the adapter.

To maintain all of your current configuration settings during an update, do not uninstall the old version of the adapter before installing the new version. Keeping the old version before installing the new version also maintains the certificate and private key. During the installation, specify the same installation directory where the previous adapter was installed. See Chapter 4, “Installing,” on page 11.

To update an existing adapter, complete the following steps:

1. 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 `setup.exe` file in the temporary directory.
3. Select the language and click **OK** to display the **Introduction** window.
4. Click **Next**.
5. Select **Update installation** and click **Next**.

   Note: The adapter must already exist if you want to perform an update installation. If it does not exist, the software generates the following message:

   ```
   Update not supported when the adapter is not previously installed.
   Cannot perform Update Installation.
   Windows Local Account Adapter is not installed on this machine.
   Please select Full Installation.
   ```

   The adapter displays the path of the adapter installation to be updated.
6. Click **OK**.

7. Review the installation settings on the pre-Installation **Summary** window.
8. Click **Install.**
9. Click **Done** on the **Install Complete** window

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

   The adapter installer updates installation of the adapter for versions 6.0 or later only.

Upgrading Windows Local Account Adapter in silent mode by using command-line parameters

You can use the -i silent option to update the adapter in silent mode.

Note: If you install adapter in silent mode, the uninstaller runs in silent mode irrespective of whether you are using -i silent option.

The installer refers to the adapter registry keys to detect if the adapter is installed on the system where you are running the command. The installer updates the adapter only if it successfully detects a prior installation of the adapter on the system. If no prior installation is found on the system, the installation ends. A log file `Tivoli_Windows_Local_Account_Adapter_SilentInstallLog` is generated.

Note: When performing an update installation the **`-DUSER_INSTALL_DIR`** parameter must not be used.

Issue one of the following commands on a single line:

- ```
  setup.exe -i silent -DLICENSE_ACCEPTED=TRUE
  -DUSER_INPUT_INSTALL_TYPE_1= -DUSER_INPUT_INSTALL_TYPE_2=\"Update Installation\"
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2=1
  ```

- ```
  setup.exe -i silent -DLICENSE_ACCEPTED=TRUE
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
  -DUSER_INPUT_INSTALL_TYPE_BOOLEAN_2=1
  ```

Upgrading Windows Local Account Adapter in silent mode by using a response file

You can use response file to provide inputs during silent installation.

1. Use one of these actions to create a response file.
   - Generate a response file by issuing the command:

     ```
     setup.exe -r "Full path of response file"
     ```

     This command runs the installer in interactive mode and installs the adapter. After the installation completes, the file specified as "*Full path of response file*" is created. The file contains the required parameters.

     Note: If you are running this command to generate only the response file, you must uninstall the adapter by using the uninstaller.
   - Manually create a response file:

     Use a text editor to create a text file. For example create a file `WinAD64InstallParameters.txt`, with the following content:

     ```
     #Has the license been accepted
     #-----------------------------
     LICENSE_ACCEPTED=TRUE

     #Select Install Type
     #-------------------
     USER_INPUT_INSTALL_TYPE=\"\",\"Update Installation\"
     USER_INPUT_INSTALL_TYPE_1=
     USER_INPUT_INSTALL_TYPE_2=Update Installation
     ```

```
USER_INPUT_INSTALL_TYPE_BOOLEAN_1=0
USER_INPUT_INSTALL_TYPE_BOOLEAN_2=1
```

2. Issue the command:

```
setup.exe -i silent -f "Full path of response file"
```

   For example:

```
setup.exe -i silent -f "C:\WinLocalInstallParameters.txt"
```

3. Restart the workstation.

   When the installation completes the adapter update, a new installation log file is created. It replaces the old file in the installation directory.

Upgrading the ADK

You can use the ADK update program to update the ADK portion of the adapters that are currently installed on a workstation. Use the update program to install just the ADK, and not the entire adapter.

The ADK consists of the runtime library, filtering, and event notification functionality, protocol settings, and logging information. The remainder of the adapter is composed of the Add, Modify, Delete, and Search functions. While all adapters have the same ADK, the remaining functionality is specific to the managed resource. As part of the ADK update, the ADK library and the DAML protocol library are updated. In addition, the **agentCfg** and certTool binary files are updated.

Note: The adapter supports upgrading the ADK from version 6.0 to newer versions 6.*x* only.

Before updating the ADK files, the update program checks the current version of the ADK. If the current level is higher than what you are attempting to install, a warning message is displayed.

To upgrade the ADK, take these steps:

1. Download the ADK upgrade program compressed file from the IBM website.
2. Extract the contents of the compressed file into a temporary directory.
3. Stop the Windows Local Account Adapter service.
4. Start the upgrade by running the installation program file in the temporary directory.

   For example, select **Run** from the **Start** menu, and type `C:\TEMP\`*`installation program`* in the **Open** field.

   If no adapter is installed, you 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 Installation Information window, click **Next** to begin the installation.
7. In 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, `ADK60Installer.log` and `ADK60Installeropt.log` files are created in the folder where you run the installation program.

Chapter 6. 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 it to function correctly.

To configure the adapter, perform the following steps:

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

1. Start the adapter service.
2. Configure the Directory Access Markup Language (DAML) protocol for the adapter to establish communication with the Identity server. See “Modifying protocol configuration settings” on page 30.
3. Configure the adapter for event notification.

   See Configuring event notification.
4. Install a certificate on the workstation where the adapter is installed and also on the Identity server to establish secure communication between them.

   See “Configuring SSL authentication” on page 46.
5. Import the adapter profile on the Identity server.
6. Configure the adapter service.
7. Use the adapter configuration program, **agentCfg**, to view or modify the adapter parameters.

   See “Starting the adapter configuration tool” on page 27.
8. Configure the adapter account form. See the IBM Security Verify Governance product documentation.
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.

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

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 7. 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

Related tasks

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

Accessing help and additional options

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

Viewing configuration settings

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

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   : FALSE
License          : NONE
Asynchronous ADD Requests  : FALSE (Max.Threads:3)
Asynchronous MOD Requests  : FALSE(Max.Threads:3)
Asynchronous DEL Requests  : FALSE (Max.Threads:3)
Asynchronous SEA Requests  : FALSE (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.

Related tasks

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

Accessing help and additional options

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

Modifying protocol configuration settings

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

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.

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)
L. MIN_TLS_LEVEL      1.0    ;Minimum TLS level (0 for none)
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 8. 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 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 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`.
D	Displays the following prompt: `Modify Property 'PORTNUMBER':` Type a different port number. This value is the port number that the 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 Identity server. This value is the DNS name or the IP address of the 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 Identity server. The adapter uses this port number to connect to the Identity server. The default port number is 9443.

Table 8. Options for the DAML protocol menu (continued)	
Option	**Configuration task**
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.
I	Displays the following prompt: `Modify Property 'VALIDATE_CLIENT_CE':` Specify TRUE for the 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 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 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 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 Verify Governance and the adapter connection. This option applies to setups that have a firewall between IBM Security Verify Governance and the adapter. This firewall has a timeout value that is less than the maximum connection age DAML property on IBM Security Verify Governance. 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 8. Options for the DAML protocol menu (continued)	
Option	**Configuration task**
L	This option controls the minimum TSL level that is used when SSL is enabled. The setting supersedes the values DISABLE_SSLV3 and DISABLE_TLS10. The valid settings for this value are: – `0`: No restrictions. This setting allows SSLV3 connections which are known to have vulnerabilities. – `1.0`: TLS 1.0 and higher are supported. – `1.1`: TLS 1.1 and higher are supported. – `1.2`: TLS 1.2 and higher are supported. – `1.3`: TLS 1.3 and higher are supported. For backward compatibility, if MIN_TLS_LEVEL is not set, it will be set at startup based on the settings of DISABLE_SSLV3 and DISABLE_TLS10.

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 49
Use the certTool utility to manage private keys and certificates.

"Configuring SSL authentication" on page 46
You can provide SSL authentication, certificates, and enable SSL authentication with the certTool utility.

Related tasks

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

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

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

Accessing help and additional options

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

"Installing the certificate" on page 52
After you receive your certificate from your trusted CA, install it in the registry of the adapter.

Changing the configuration key

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

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.

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

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

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

Changing `activity logging` settings

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

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

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

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.
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.

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

Related tasks

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

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

Modifying protocol configuration settings

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

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

Modifying registry settings

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

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.

Related tasks

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

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

Accessing help and additional options

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

Modifying non-encrypted registry settings

You can modify the non-encrypted registry settings.

To modify the non-encrypted registry settings, complete the following steps:

1. At the Agent Registry Menu, type A to display the Non-encrypted Registry Settings Menu:

```
Agent Registry Items
--------------------------

01. ManageHomeDirs                    'FALSE'
02. ReconBufferSize           '-1'
03. ReconHomeDirSecurity      'FALSE'
04. UnlockOnPasswordChange    'FALSE'
-------------------------------
           Page 1 of 1

A. Add new attribute
B. Modify attribute value
C. Remove attribute

X. Done

Select menu option:
```

2. Type the menu letter for the action that you want to perform on an attribute.

Table 10. Attribute configuration option descriptions

Option	Configuration task
A	Add new attribute
B	Modify attribute value
C	Remove attribute

3. Type the registry item name, and press **Enter**.
4. If you selected option A or B, type the registry item value and press **Enter**.

   The non-encrypted registry settings menu reappears and displays your new settings.

Table 11. Registry key descriptions

Key	Description
ManageHomeDirs	Specifies whether the adapter creates the home directory for the user. If this key is set to TRUE, the adapter creates the home directory for the user. If this key is set to FALSE, the adapter updates only the home directory information for the user account. A physical home directory is not created. The default value is TRUE.

Table 11. Registry key descriptions (continued)	
ReconBufferSize	Specifies the size of the buffer that is used by adapter to hold user information in memory during RECON. If you specify `-1`, the adapter allocates the memory required to hold all of the user information. If you specify a different value (based on the number of 8-bit bytes) the adapter holds a limited amount of user information. In this case, the adapter sends multiple requests to the Windows server to get the information for the users. The default value is `-1`.
ReconHomeDirSecurity	Specifies whether the RECON operation specifies the NTFS access information for the user. If this key is set to TRUE, the adapter returns the NTFS access information during a reconciliation for the user. The default value is `False`.
UnlockOnPasswordChange	If this key is set to TRUE: • The adapter changes the account lock status after a password change operation. • The adapter also unlocks the user account, when a password change is requested for a user account which is locked. The default value is FALSE.

Related tasks

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

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

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

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings

You can change the code page settings for the adapter.

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

Modifying advanced settings

You can change the adapter thread count settings.

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:

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 12. 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.

Table 12. Options for advanced settings menu (continued)	
Option	**Description**
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
Start the **agentCfg** tool to access the configuration menu, where you can modify the different adapter parameters.

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

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

Viewing statistics

You can view an event log for the adapter.

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**.

Related tasks

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

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Modifying code page settings
You can change the code page settings for the adapter.

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

Modifying code page settings

You can change the code page settings for the adapter.

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
```

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

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

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

Accessing help and additional options

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

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

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 13. 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.
-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.

*Table 13. Arguments and descriptions for the **agentCfg** help menu (continued)*	
Argument	**Description**
-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 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.

Related tasks

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

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

Modifying protocol configuration settings
The adapter uses the DAML protocol to communicate with the Identity server.

Changing the configuration key

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

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

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

Modifying non-encrypted registry settings
You can modify the non-encrypted registry settings.

Modifying advanced settings
You can change the adapter thread count settings.

Viewing statistics
You can view an event log for the adapter.

Modifying code page settings
You can change the code page settings for the adapter.

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 Identity server or from the adapter. The 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 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 Identity server.

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

Related concepts
"Overview of SSL and digital certificates" on page 2
In an enterprise network deployment, you must provide secure communication between the Identity server and the software products and components with which the server communicates.

Configuring certificates for SSL authentication

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

Use the certTool utility for these tasks:

- "Configuring certificates for one-way SSL authentication" on page 46
- "Configuring certificates for two-way SSL authentication" on page 47
- "Configuring certificates when the adapter operates as an SSL client" on page 48

Configuring certificates for one-way SSL authentication

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

Client authentication is not set on either application. The 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 Identity server. The Identity server uses the installed CA certificate to validate the certificate that is sent by the adapter.

In Figure 1 on page 47, Application A operates as the Identity server, and Application B operates as the adapter.

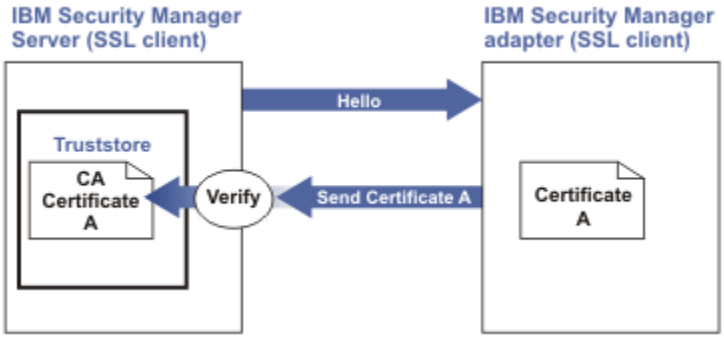

Figure 1. One-way SSL authentication (server authentication)

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

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:
      i) 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.
      ii) 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 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 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 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 Identity server.

Related tasks

"Starting certTool" on page 49
To start the certificate configuration tool named certTool for the adapter, complete these steps:

Configuring certificates for two-way SSL authentication

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

The adapter uses client authentication. After the adapter sends its certificate to the server, the adapter requests identity verification from the 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 Identity server operates as Application A and the adapter operates as Application B.

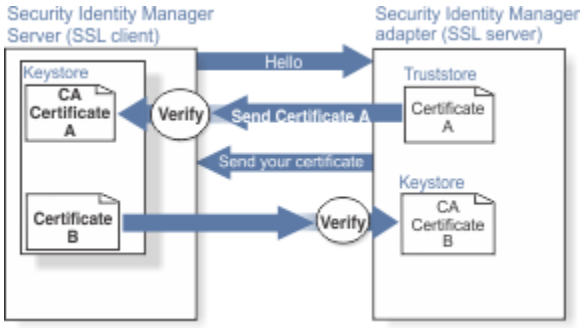

Figure 2. Two-way SSL authentication (client authentication)

Before you do the following procedure, configure the adapter and 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 Identity server.

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

1. On the 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 Identity server to the adapter.

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.

Related tasks

"Configuring certificates for one-way SSL authentication" on page 46
In this configuration, the 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.

This configuration applies if the adapter initiates a connection to the web server (used by the 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 on page 48 describes how the adapter operates as an SSL server and an SSL client.
To communicate with the Identity server, the adapter sends its certificate for authentication. To communicate with the web server, the adapter receives the certificate of the web server.

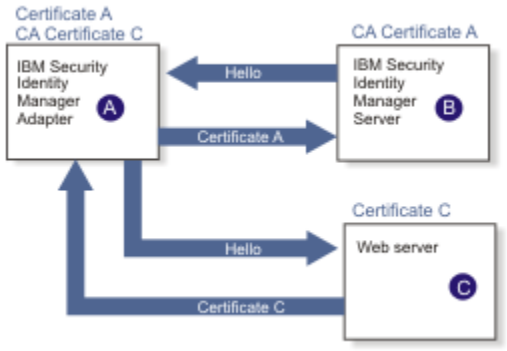

Figure 3. Adapter operating as an SSL server and an SSL client

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:

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.

You can have the software send an event notification when the adapter initiates a connection to the web server (used by the 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:

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:
```

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 Identity server.

E. List CA certificates
Show the installed CA certificates. The adapter communicates only with 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 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 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.

Related concepts

"View of the installed certificate" on page 52
To list the certificate on your workstation, type D at the Main menu of certTool.

Related tasks

"Generating a private key and certificate request" on page 51
A certificate signing request (CSR) is an unsigned certificate that is a text file.

"Installing the certificate" on page 52
After you receive your certificate from your trusted CA, install it in the registry of the adapter.

"Installing the certificate and key from a PKCS12 file" on page 52
If the certTool utility did not generate a CSR to obtain a certificate, you must install both the certificate and private key.

"Installing a CA certificate" on page 52
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.

"Deleting a CA certificate" on page 53
You can delete a CA certificate from the adapter directories.

"Viewing registered certificates" on page 53

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

"Registering a certificate" on page 53
You can register a certificate for the adapter.

"Unregistering a certificate" on page 54
You can unregister a certificate for the adapter.

"Exporting a certificate and key to a PKCS12 file" on page 54
You can export a certificate and key to a PKCS12 file.

Generating a private key and certificate request

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

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.

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.

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 a 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.

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_nameAgent\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.

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.

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

   For Windows operating systems:

   ```
   C:\Program Files\IBM\ISIM\Agents\adapter_nameAgent\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**.

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

View of the 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.

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.

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

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

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.

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**.

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.

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.

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**.

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.

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**.

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.

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**.

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 Windows Local Account Adapter JAR file, `WinLocalProfile.jar`, to change the adapter schema, account form, service form, and profile properties.

To make updates, extract the files from the JAR file, change the necessary files, and repackage the JAR file with the updated files.

Complete these steps to customize the Windows Local Account Adapter profile:

1. Copy the JAR file to a temporary directory and extract the files. See “Copying the WinLocalProfile.jar file and extracting the files” on page 55.
2. Make the appropriate file changes.
3. Install the new attributes on the Identity server. See “Creating a JAR file and installing the new attributes on the IBM Security Verify Governance Identity Manager server” on page 56.

Copying the WinLocalProfile.jar file and extracting the files

The profile JAR file, `WinLocalProfile.jar`, is included in the Windows Local Account Adapter compressed file that you downloaded from the IBM web site.

The `WinLocalProfile.jar` file contains the following files:

- `CustomLabels.properties`
- `erWinLocalAccount.xml`
- `erWinLocalDAMLService.xml`
- `resource.def`
- `schema.dsml`

You can modify these files to customize your environment.

Perform the following steps to modify the `WinLocalProfile.jar` file:

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

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

   The **`jar`** command creates the `c:\temp\WinLocalProfile` directory.
5. Edit the appropriate file.

When you finish updating the profile JAR file, install it on the Identity server. See Importing the adapter profile.

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`.

If you edit an MS-DOS ASCII file on the UNIX operating system, you see character *^M* at the end of each line. This character 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 a text editor, such as the vi editor, that ignores the *^M* character. Enter the *^M* (or Ctrl-M) in the command by pressing *^v^M* (or Ctrl V Ctrl M) in sequence.

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
   ```

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

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

After you modify the `schema.dsml` and `CustomLabels.properties` files, you must put the changes into effect. Import these files and any other files in the profile that were modified for the adapter, into the IBM Security Verify Governance Identity Manager server.

To install the new attributes, complete the following steps:

1. Create a JAR file by running the following commands:
   - Windows operating systems:

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

     The command creates the JAR file in the \TEMP directory.
   - UNIX based operating systems:

     ```
     #cd /tmp
     jar -cvf WinLocalProfile.jar WinLocalProfile
     ```

     The command creates the JAR file in the `/tmp` directory.
2. Import the `WinLocalProfile.jar` file into the IBM Security Verify Governance Identity Manager server.

   See Importing the adapter profile.
3. Stop and start the IBM Security Verify Governance Identity Manager server.

   Note: If you are updating an existing adapter profile, the new adapter profile schema is not immediately used. Stop and start the IBM Security Verify Governance Identity Manager server to refresh the cache and the adapter schema. See "Upgrading the Windows Local Account Adapter" on page 23.

Managing passwords when you restore accounts

When accounts for a person are restored after a previous suspension, you are not prompted to supply a new password for the reinstated accounts. However, there are circumstances when you might want to circumvent this behavior.

The password requirement to restore an account on Windows 2008, and Windows 7 servers 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 reject a password when a request is made to restore an account. In this case, you can configure IBM Security Verify Governance Identity Manager to forego the new password requirement. Your company might have a business process in place that dictates that the account restoration process must be accompanied by resetting the password. You can set the Windows Local Account 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 identify whether you discard a password that a user enters when multiple accounts on disparate resources are being restored. In this scenario, only some of the restored accounts require a password. Remote services discard the password from the restore action for those managed resources that do not require them.

Note: If you are upgrading an existing adapter profile, the new adapter profile schema is not immediately available. Stop and start the IBM Security Verify Governance Identity Manager to refresh the cache and the adapter schema. See "Upgrading the Windows Local Account Adapter" on page 23.

To configure the Windows Local Account Adapter to prompt for a new password when restoring accounts:

1. Stop the IBM Security Verify Governance Identity Manager.
2. Extract the files from the `WinLocalProfile.jar` file.

   See "Copying the WinLocalProfile.jar file and extracting the files" on page 55.
3. Change to the `\WinLocalProfile` 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 = "FALSE"/>
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
PASSWORD_NOT_ALLOWED_ON_RESTORE" Value = "FALSE"/>
```

   Adding the two options in the example ensures that you *are prompted* for a password when an account is restored.
5. Create a `WinLocalProfile.jar` file with the `resource.def` file and import the adapter profile file into the IBM Security Verify Governance Identity Manager server.

   See "Creating a JAR file and installing the new attributes on the IBM Security Verify Governance Identity Manager server" on page 56.
6. Start the IBM Security Verify Governance Identity Manager again.

Configuring Local Groups attributes with replace attribute

The default behavior for attribute **`erNTLocalGroups`** (Local Groups) has changed to `add` and `delete` rather than `replace`. This change does not impact any IBM Security Verify Governance Identity Manager provisioning polices or account defaults. The default behavior change ensures that the adapter does not overwrite any Local Groups changes made locally.

Follow this procedure to change back the default behavior to `replace`.

1. Open the `resounce.def` file in the `WinlocalProfile.jar` adapter profile.
2. Make sure that the `ReplaceMultiValue` attribute value is `true`. For example:

```
<Parameter Name="erNTLocalGroups" Source="account" ReplaceMultiValue="true" />
```

Verifying that the adapter is working correctly

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

1. Test the connection for the service that you created on Identity server.
2. Perform a full reconciliation from the Identity server.
3. Perform all supported operations such as add, modify, and delete on one user account.
4. Examine the `WinLocalAgent.log` file after each operation to ensure that no errors were reported.

Chapter 7. 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 Windows Local Account Adapter is installed on your system.

Table 14. Warning and error messages

Warning or error message	Possible cause	Corrective action
The user name could not be found.	A request was made to either modify, suspend, restore, or delete a user account that does not exist on the managed resource.	Perform a reconciliation operation to ensure that the user exists on the managed resource and is not directly deleted or modified on the managed resource.
The user account already exists.	This error occurs when a request is made to add a user account that exists.	Create a user account with another user ID. For information about creating a user account, see the IBM Security Verify Governance product documentation.
Error removing home directory.	This error occurs when: • The **Remove Home Directory** check box is not selected on the account form. • The value of the **Home Directory** attribute is not cleared.	Perform the following steps on the account form: • Select the **Remove Home Directory** check box. • Clear the value of the **Home Directory** attribute.
Error setting user attributes.	This error occurs when a request is made to either add or modify a user account without correct values specified for the optional account form attributes.	Ensure that you specified appropriate values to the optional attributes on the account form.
Error enumerating user accounts.	This error occurs when a reconciliation operation is performed and the required administrative access rights are not provided to the user on the managed resource.	Ensure that the user has the required administrative access rights on the managed resource to perform the reconciliation operation.
The group already exists	This error occurs when a request is made to add a new group that already exists on the managed resource.	Create a group with a unique name.
Group not found.	This error occurs when an attempt is made to add a user to a group that does not exist on the managed resource.	Perform a reconciliation operation to verify whether the group exists on the managed resource.
User is already a member of Group.	The user is already a member of the group specified.	The user is already a member of the local group that is specified on the account form. No action is required.

Table 14. Warning and error messages (continued)

Warning or error message	Possible cause	Corrective action
The password is too short.	This error occurs when the user account password does not comply to the password policy requirements.	Check the minimum password length, password complexity, and password history requirements. Ensure that the: • Password meets the minimum required length. • Password is complex. • Password meets the password policy requirements. For more information about the password policy, see the Local Security settings on the managed resource.
Error creating a user. Error: 5 - Access is denied.	This error occurs when an attempt is made to add a user on the managed resource, however, the user does not have the required administrative rights.	Ensure that the user account used by the adapter service has the required administrative rights on the managed resource to perform the add operation.
Error deleting a user. Error: 5 - Access is denied.	This error occurs when an attempt is made to delete a user on the managed resource, however, the user does not have the required administrative rights.	Ensure that the user account used by the adapter service has the required administrative rights on the managed resource to perform the delete operation.
The network path was not found.	This error occurs in the following situations: • The specified network path is incorrect. • The specified server name is unavailable in the network.	Ensure that: • The network path specified on the account form is correct. For example, when you want to create a home directory, then provide the path in the following format on the account form: `\\servername\sharename\foldername` **Note:** The Windows Local Account Adapter supports creation and deletion of only Universal Naming Conventions (UNC) home directories. Specify the UNC home directory path in the following format: `\\servername\sharename\foldername` • Ensure that the server name exists on the managed resource.

Chapter 8. Uninstalling

To remove an adapter from the 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 Identity server.

Before you remove the adapter, inform your users that the adapter is unavailable. If the server is taken offline, adapter requests that were completed might not be recovered when the server is back online.

Uninstalling the adapter from the target server

The adapter has an uninstall utility that you can use to remove the adapter from the target server.

1. Stop the adapter service.
2. Run the uninstaller.
   a) Navigate to the adapter home directory.
      For example, `C:\Program Files\IBM\ISIM\Agents\`*`adaptername`*`\_uninst`.
   b) Double-click the `uninstaller.exe` file.
   c) Click **Uninstall**.
   d) In the uninstallation **Summary** window, click **Done**.
3. Inspect the directory tree for the adapter directories, subdirectories, and files to verify that uninstall is complete.

Deleting the adapter profile

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

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

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

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

Chapter 9. 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 Identity server communicates with the adapter by using attributes, which are included in transmission packets that are sent over a network.

Table 15. Attributes, descriptions, and corresponding data types

Attribute	Directory server attribute	Description	Data format
LocalName	erNTLocalName	Specifies the name for a local group	String
GroupComment	erNTGroupComment	Specifies the comment attribute for groups	String
GroupType	erNTGroupType	Specifies the group type	String
HomeDirNtfsAccess	erNTHomeDirNTFSAccess	Specifies the NTFS security to be applied to the home directory	String
HomeDirRemove	erNTHomeDirRemove	Specifies the special attribute which, if TRUE, instructs the adapter to delete a UNC home directory and its contents when the UserHomeDir attribute is being deleted	Boolean
LOCALGROUP	erNTLocalGroups	Specifies the local group that the user is member	String
UserAcctExpires	erNTExpirationDate	Specifies the account expiration date	Integer
UserBadPWCount	erNTUserBadPWCount	Specifies the number of allowed logon attempts with an invalid password	Integer
UserCantChangePassword	erNTCantChangePassword	Specifies whether the user can change their password. This value cannot be set to TRUE if UserPasswordExpired is set to TRUE.	Boolean
UserCodePage	erNTCodePage	Specifies the language for the code page	Integer
UserCountryCode	erNTUserCountryCode	Specifies the country code	Integer
UserComment	description	Specifies a user comment	String
UserFullName	cn	Specifies the full name of the user	String
UserHomeDir	erNTHomeDir	Specifies the home directory for the user	String

Table 15. Attributes, descriptions, and corresponding data types (continued)

Attribute	Directory server attribute	Description	Data format
UserHomeDirDrive	erNTHomeDirDrive	Specifies the drive letter used to map UNC home directory. Required for UNC Home Directory.	
UserHomeDirRequired	erNTHomeDirRequired	Specifies whether the home directory is required	Boolean
UserLastLogoff	erNTLastLogoff	Specifies the time of the last logoff	Integer
UserLastLogon	erLastAccessDate	Specifies the time of the last logon	Integer
UserLockedOut	erNTLockedOut	Specifies whether the account is locked out. This value must be set to FALSE.	Boolean
UserLogonHours	erLogonTimes	Specifies the time during which the user can logon	String
UserName	eruid	Specifies the user account name	String
UserNumLogons	erNumLogons	Specifies the number of times that the user logged on successfully	Integer
UserPassword	erPassword	Specifies the account password	String
UserPasswordAge	erNTPasswordAge	Specifies the number of seconds since the last password change	Integer
UserPasswordExpired	erNTPasswordExpired	Specifies whether the password has expired. If this value is set to TRUE, you cannot set UserCantChangePassword to TRUE.	Boolean
UserPasswordNeverExpires	erNTPasswordNeverExpires	Specifies whether the password will expire	Boolean
UserPasswordNotRequired	erNTPasswordNotRequired	Specifies whether a password is required	Boolean
UserProfile	erNTProfile	Specifies the path to the user profile	String
UserScriptPath	erNTScriptPath	Specifies the path to the user logon script file	String
UserStatus	erAccountStatus	Specifies the status of the user account	Boolean
UserUsrComments	erNTUsrComment	Specifies a comment	String
ServerName	erWinLocalServer	Specifies the name of the managed resource to connect to.	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 16. Add request attributes

Required attribute	Optional attribute
erUid	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 17. Change request attributes

Required attribute	Optional attribute
erUid	All other supported attributes

System Login Delete

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

Table 18. Delete request attributes

Required attribute	Optional attribute
erUid	None

System Login Suspend

A System Login Suspend is a request to disable a user account.

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

Table 19. Suspend request attributes

Required attribute	Optional attribute
erUid erAccountStatus	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 using the same attributes as the ones before the Suspend function was called.

Table 20. Restore request attributes	
Required attribute	**Optional attribute**
erUid erAccountStatus	None

Reconciliation

The Reconciliation function synchronizes user account information between IBM Security Verify Governance and the adapter.

Table 21. Reconciliation attributes	
Required attribute	**Optional attribute**
None	None

Special attributes

Certain attributes have special syntax and meaning that customers needs to be aware off. This information will be used to help the customer in how to supply the attribute value.This topic is not applicable for this adapter.

Index

A

C

D

E

H

I

K

L

O

P

R

S

T

U

V