IBM Security Verify Identity
7.0

IBM i 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 IBM i Adapter enables communication between the Identity server and an IBM i system.

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 adapter automates several administrative and management tasks.

The adapter automates the following user account management tasks:

- Reconciling user accounts and other support data
- Adding user accounts
- Modifying user account attributes
- Modifying user account passwords
- Suspending, restoring, and deleting user accounts

Architecture of the adapter

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

You must install the following components:

- The Dispatcher
- The Security Directory Integrator connector
- IBM® Security Verify Adapter profile

You need to install the RMI Dispatcher and the adapter profile; however, the Security Directory Integrator connector might already be installed with the base Security Directory Integrator product.

A directory server is installed by default on the IBM i operating system. All users provisioned on the IBM i operating system are projected as directory entries on this directory server. The Security Directory Integrator LDAP connector communicates with the directory server on the IBM i operating system to perform user account management operations.

Figure 1 on page 2 describes the components that work together to complete the user account management tasks in a Security Directory Integrator environment.

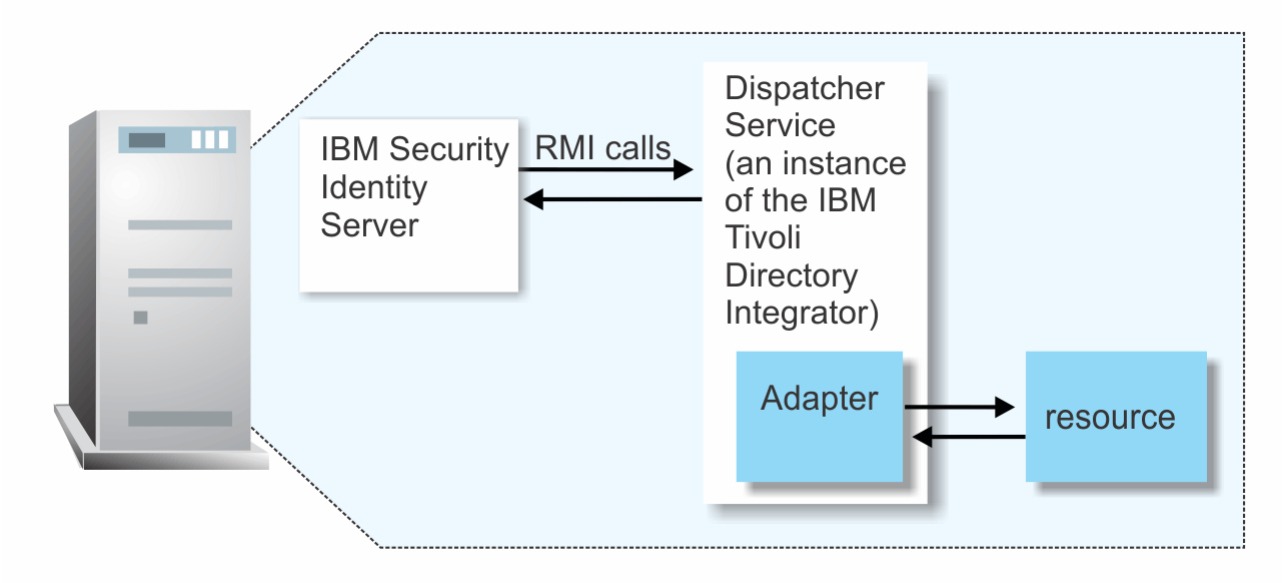

Figure 1. The architecture of the IBM i Adapter

Supported configurations

The adapter supports both single and multiple server configurations.

The fundamental components in each environment are:

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

The adapter must reside directly on the server running the Security Directory Integrator server.

Single server configuration

In a single server configuration, install the Identity server, the Security Directory Integrator server, and the IBM i Adapter on one server to establish communication with the IBM i system with a directory server interface. The IBM i system is installed on a different server as described in Figure 2 on page 2.

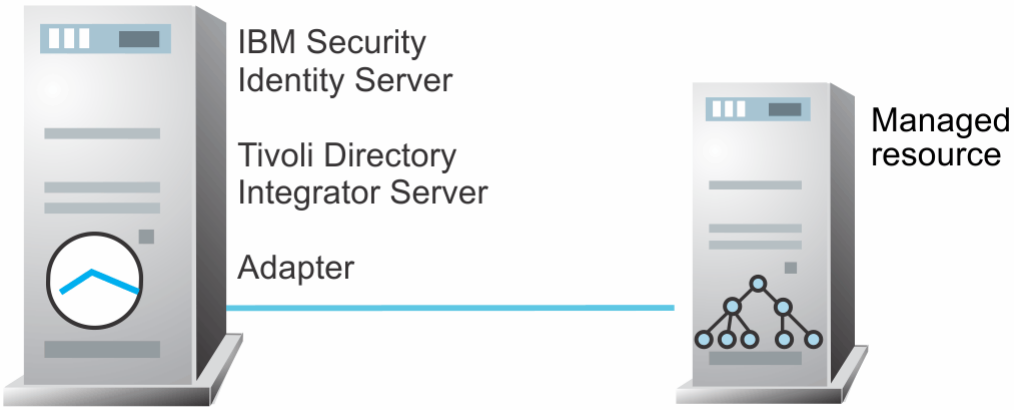

Figure 2. Example of a single server configuration

Multiple server configuration

In a multiple server configuration, the Identity server, the Security Directory Integrator server, the IBM i Adapter, and the IBM i system are installed on different servers. Install the Security Directory Integrator server and the IBM i Adapter on the same server as described in Figure 3 on page 3.

Figure 3. Example of multiple server configuration

Chapter 2. Planning

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

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x

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

Upgrade

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

Configuration

Complete these tasks.

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

Troubleshooting

See the following topics.

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

Uninstallation

Complete these tasks.

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

Reference

See the following topics.

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

Related concepts

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

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

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.

Prerequisites

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

Table 1 on page 6 identifies the software and operating system prerequisites for the adapter installation.

Ensure that you install the adapter on the same workstation as the Tivoli® Directory Integrator server.

Table 1. Requirements to install the adapter

Prerequisite	Description

Table 1. Requirements to install the adapter (continued)	
System	• A supported hardware system. – i5/OS V5R4 – IBM i V6R1 – IBM i V7R1 • A minimum of 16 MB of memory. • A minimum of at least 20 MB of free disk space.
Software	**i5/OS V5R4** • 5722SS1, option 12 (Host Servers) • 5722JC1 (IBM Toolbox for Java™) The following software is required for secure connections: • 5722SS1, option 34 (Digital Certificate Manager) • 5722AC3 - V5R3 only (Crypto Access Provider 128-bit) • 5722DG1 (IBM HTTP Server) The following administrative tool is needed for the directory server: iSeries Navigator - included with iSeries Access EZSetup **IBM i 7.1** • 5770SS1, option 12 (Host Servers) • 5761JV1 (IBM Developer Kit for Java) The following software packages are required for secure connections: • 5770SS1, option 34 (Digital Certificate Manager) • 5770SSI, option 35, (CCA Cryptographic Service Provider) • 5770DG1 (IBM HTTP Server for i) The following administrative tool is needed for IBM Directory Server for i configuration and the Digital Certificate Manager: 5770XH2 - IBM Navigator for i (included in IBM i Access)
Network connectivity	The adapter must be installed on a system that can communicate with the IBM Security Verify Identity service through the TCP/IP network.
System Administrator authority	A user profile with the following privileges is needed for the installation: User class=*SECOFR, SPCAUT=*USRCLS,*SECADM,*ALLOBJ.

Table 1. Requirements to install the adapter (continued)	
Directory Integrator	• IBM Security Directory Integrator Version 7.1.1 + 7.1.1-TIV-TDI-FP0004 + 7.2.0-ISS-SDI-LA0008 • IBM Security Directory Integrator Version 7.2 **Note:** • Earlier versions of IBM Security Directory Integrator that are still supported might function properly. However, to resolve any communication errors, you must upgrade your Directory Integrator release to the versions that the adapter officially supports. • The adapter supports IBM Security Directory Integrator 7.2, which is available only to customers who have the correct entitlement. Contact your IBM representative to find out whether you have the entitlement to download IBM Security Directory Integrator 7.2.
Identity server	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

For information about the prerequisites and supported operating systems for Security Directory Integrator, see the *IBM Security Directory Integrator 7.1: Administrator Guide*.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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.

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 Identity Download Document* for instructions.

Note:

You can also obtain additional adapter information from IBM Support.

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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.

Installation worksheet

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

Table 2. Required information to install the adapter

Required information	Description	Value
Security Directory Integrator Home Directory	The *ITDI_HOME* directory contains the `jars/connectors` subdirectory that contains adapter jars.	If Security Directory Integrator version 7.1 is automatically installed, the default directory path depends on the operating system. **Windows** *drive*`\Program Files\IBM\TDI\V7.1` **UNIX** `/opt/IBM/TDI/V7.1`
Solution Directory	When you install the dispatcher, the adapter prompts you to specify a file path for the solution directory. For more information about the solution directory, see the *Dispatcher Installation and Configuration Guide*.	The default solution directory for version 7.1 depends on the operating system. **Windows** *drive*`\Program Files\IBM\TDI\V7.1\`*timsol* **UNIX** `/opt/IBM/TDI/V7.1/`*timsol*

Related concepts

Roadmap for IBM Security Directory Integrator based adapters, for IBM Security Verify Identity 7.x
Follow this section when using the guide to install, configure, troubleshoot, or uninstall the adapter.

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

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

Chapter 3. Installing

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

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

Depending on your adapter, the Security Directory Integrator connector might already be installed as part of the Security Directory Integrator product and no further action is required. If the connector is not pre-installed, install it after the Dispatcher.

Installing the dispatcher

If this is the first Security Directory Integrator-based adapter installation, you must install the RMI Dispatcher before you install the adapter. Install the RMI Dispatcher on the same Security Directory Integrator server where you want to install the adapter.

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

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

Installing the adapter binaries or connector

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

Before you begin

- The Dispatcher must be installed.

About this task

The adapter uses the IBM Security Directory Integrator JDBC connector. Follow the steps in the procedure to to download and copy the JDBC Connector JAR. As such, you just need to install the Dispatcher. See the *IBM Security Dispatcher Installation and Configuration Guide*..

Restarting the adapter service

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

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

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

Importing the adapter profile

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

Before you begin

- You have root or 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.The JAR file for IBM Security Identity Manager is located in the top level folder of the installation package.

About this task

Service definition files are also called adapter profile files.

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

Procedure

1. Log on to the Identity server by using an account that has the authority to perform administrative tasks.
2. From the navigation tree, select **Configure System** > **Manage Service Types**.

   The **Manage Service Types** page is displayed.
3. On the **Manage Service Types** page, click **Import**.

   The **Import Service Type** page is displayed.
4. On the **Import Service Type** page, complete these steps:
   a) In the **Service Definition File** field, type the directory location of the *<Adapter>*`Profile.jar` file, or click **Browse** to locate the file.
   For example, if you are installing the IBM Security Verify Adapter for a Windows server that runs Active Directory, locate and import the `ADProfileJAR` file.
   b) Click **OK** to import the file.

Results

A message indicates that you successfully submitted a request to import a service type.

What to do next

- The import occurs asynchronously, which means it might take some time for the service type to load into the Identity server from the properties files and to be available in other pages. On the **Manage Service Types** page, click **Refresh** to see the new service type. If the service type status is `Failed`, check the log files to determine why the import failed.
- If you receive a schema-related error, see the `trace.log` file for information about it. The `trace.log` file location is specified by the **`handler.file.fileDir`** property that is defined in the `enRoleLogging.properties` file. The `enRoleLogging.properties` file is in the Identity server*HOME*`\data` directory. .

Configuring the Directory Server

The LDAP Directory Server is part of the IBM i operating system. By default, the directory server is configured to start a non-secured service automatically.

About this task

For additional customization, you must install the iSeries Navigator software, if this is not already installed and you must use this software. For specific instructions about installing the software, see the EzSetup CD included with the operating system bundle.

Note: When you install the iSeries Navigator software on your system, you must install all features. The typical installation option does not install the Network feature.

To start the Directory Server Configuration wizard:

Procedure

1. Locate the connection to the iSeries system.

   If a connection does not exist, you must create a connection.
2. Expand the **Network** folder for the system.
3. Expand **Servers**.
4. Click **TCP/IP**.
5. Right-click **IBM Directory** service, and select **Properties**.
6. Ensure that the **Start server when TCP is started** check box is checked.
7. From the Database/Suffixes window, locate the **System Objects Suffix** field.

   The suffix information is required to complete the "User Container Base DN" while you are creating the IBM i service.

   Note: The system objects suffix is RDN of the os400-root object class.

   ```
   RDN: os400-sys=<my400server.ibm.com>
   Objectclass = os400-root
   ```

   See Creating an adapter service/target.
8. Ensure that the **Allow system object updates** check box is checked.
9. Click the **Network** tab. In the **Connections to allow** field, locate the ports used for the directory server.

   The default port for a non-secured connection is 389 and the default port for a secure connection is 636. Ensure that **Server Authentication** is selected.

   Note:

   - The SSL Directory service is not enabled until a certificate is assigned to the service. See "Configuring certificates for one-way SSL authentication" on page 24 for more information about SSL authentication.
   - If your system is being used as a Lotus® Notes® Domino® LDAP server, ensure that you specify different port numbers so that each server has unique ports for SSL and non-SSL services.
10. Click **OK**.

Creating an adapter service/target

After you import the adapter profile on the Identity server, create a service/target so that Identity server can communicate with the managed resource.

Before you begin

Complete "Importing the adapter profile" on page 12.

About this task

You must create an administrative user account for the adapter on the managed resource. You can provide the account information such as administrator name and password when you create the adapter service. Ensure that the account has sufficient privileges to administer the users. For information about creating an administrative account, see the documentation for the managed resource.

To create or change a service, you must use the service form to provide information for the service. Service forms might vary depending on the adapter. The service name and description that you provide for each service are displayed on the console. Therefore, it is important to provide values that make sense to your users and administrators.

Procedure

1. From the navigation tree, click **Manage Services**.
   The **Select a Service** page is displayed.
2. On the **Select a Service** page, click **Create**.
   The **Create a Service** wizard is displayed.
3. On the **Select the Type of Service** page, click **Search** to locate a business unit.
   The **Business Unit** page is displayed.
4. On the **Business Unit** page, complete these steps:
   a) Type information about the business unit in the **Search information** field.
   b) Select a business type from the **Search by** list, and then click **Search**.
      A list of business units that matches the search criteria is displayed.

      If the table contains multiple pages, you can do the following tasks:

      - Click the arrow to go to the next page.
      - Type the number of the page that you want to view and click **Go**.

   c) In the **Business Units** table, select business unit in which you want to create the service, and then click **OK**.
      The **Select the Type of Service** page is displayed, and the business unit that you specified is displayed in the **Business unit** field.
5. On the **Select the Type of Service** page, select a service type, and then click **Next**.

   If the table contains multiple pages, you can do the following tasks:

   - Click the arrow to go to the next page.
   - Type the number of the page that you want to view and click **Go**.
6. On either the **Service Information** or **General Information** page, specify the appropriate values for the service instance.
   The content of the **General Information** page depends on the type of service that you are creating. The creation of some services might require more steps.
7. To create a service with NTLM authentication, the administrator login is in the following format:

   ```
   <Domain Name>\<Login Name>
   ```
8. For NLTM authentication, select **Authentication** mode as 'Claims-Based Authentication.
9. On the **Dispatcher Attributes** page, specify information about the dispatcher attributes, and then click **Next** or **OK**.
   The **Dispatcher Attributes** page is displayed only for IBM Security Directory Integrator based services.
10. Optional: On the **Access Information** page, select the **Define an Access** check box to activate the access definition fields. Select the type of access you want to enable.

Specify the expected access information and any other optional information such as description, search terms, more information, or badges.

11. On the **Status and Information** page, view information about the adapter and managed resource, and then click **Next** or **Finish**.

    The adapter must be running to obtain the information.

12. On the **Configure Policy** page, select a provisioning policy option, and then click **Next** or **Finish**.

    The provisioning policy determines the ownership types available for accounts. The default provisioning policy enables only Individual ownership type accounts. Additional ownership types can be added by creating entitlements on the provisioning policy.

    Note: If you are creating a service for an identity feed, the **Configure Policy** page is not displayed.

13. Optional: On the **Reconcile Supporting Data** page, either do an immediate reconciliation for the service, or schedule a supporting data reconciliation, and then click **Finish**.

    The **Reconcile Supporting Data** page is displayed for all services except for identity feed services.

    The **supporting data only** reconciliation option retrieves only the supporting data for accounts. The supporting data includes groups that are defined on the service. The type of supporting data is defined in the adapter guide.

14. Optional: On the **Service Information** or **General Information** page, click **Test Connection** to validate that the data in the fields is correct, and then click **Next** or **Finish**.

    If the connection fails, contact the analyst who is responsible for the computer on which the managed resource runs.

Results

A message is displayed, indicating that you successfully created the service instance for a specific service type.

Service/Target form details

Complete the service/target form fields.

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

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

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

IBM Security Directory Integrator location

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

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

URL
Specify the location and port number of the directory server on the IBM i system. Valid syntax is `ldap://ip-address:port`, where *ip-address* is the IBM i server host and *port* is the IBM i LDAP port number. For example, you might specify the URL as `ldap://irvas02.eng.irvine.ibm.com:389`.

If SSL is enabled then the syntax is `ldaps://ip-address:SSLPort`. For example, you might specify the URL as `ldaps://irvas02.eng.irvine.ibm.com:636`.

See "Configuring the Directory Server" on page 13 for information about setting the LDAP port.

Administrator name
Specify the iSeries User ID. The user profile must have *SECADM, *ALLOBJ special authorities. See "Prerequisites" on page 6.

Password
Specify the password for the administrator name.

User container Base DN
Specify the distinguished name (DN) of the container or base point where the user profiles are stored. The adapter creates new users under this DN. Also, search operations return user account entries under this DN. For example, you might specify the DN as `cn=accounts,os400-sys=irvas02.eng.irvine.ibm.com`. For more information about setting the Base DN value for the target iSeries system, see "Configuring the Directory Server" on page 13.

Use SSL communication with LDAP
This check box is used to specify whether SSL authentication is to be used between Security Directory Integrator and the IBM i Directory Server. For more information about SSL authentication, see "Configuring certificates for one-way SSL authentication" on page 24.

Value of OWNOBJOPT parm for delete
Specify the type of operations that are being done on the owned objects of the user profile that is being deleted. This field is a text field and can be one of the following values:

***NODLT**
If the user owns any objects other than the message queue associated with the user profile, the owned objects for the user profile do not change. The user profile is not deleted. If the user owns only the message queue associated with the profile, then the message queue and the profile are deleted.

***DLT**
The objects owned by the user profile are deleted. If the deletion of the objects is successful, the user enrollment information is removed from OfficeVision*.

CHGOWN *username
The owned objects for the user profile have ownership transferred to the user profile specified in *username*. If the transfer of all owned objects is successful, the user profile is deleted.

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

AL FileSystem Path
Specify the file path from where the dispatcher loads the assembly lines. If you do not specify a file path, the dispatcher loads the assembly lines received from Identity server. For example, you can specify the following file path to load the assembly lines from the `profiles` directory of the Windows operating system: *drive*`:\Program Files\IBM\TDI\V7.0\profiles` or you can specify the following file path to load the assembly lines from the `profiles` directory of the UNIX and Linux® operating system: `/opt/IBM/TDI/V7.0/profiles`

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

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 requests to the managed resource.

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

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

Dispatcher version
Specifies the version of the Dispatcher.

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

Adapter account
Specifies the account that runs 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.

Note: If the following fields on the service form are changed for an existing service, restart the adapter service on the Security Directory Integrator server.

- **User container Base DN**
- **Use SSL communication with LDAP**
- **Value of OWNOBJOPT parm for delete**
- **Max Connection Count**

Installing the adapter language package

The adapters use a separate language package from IBM Security Verify Identity.

See *Installing the adapter language pack* from the IBM Security Verify Identity product documentation.

Verifying that the adapter is working correctly

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

Procedure

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

Related concepts
Password management when restoring accounts

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account. However, in some cases you might not want to supply a new password.

Related tasks

Customizing the adapter profile

To customize the adapter profile, you must modify the IBM i Adapter JAR file, `IDIOS400profile.jar`. You might customize the adapter profile to change the account form or the service form.

Chapter 4. Upgrading

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

To verify the required version of these adapter components, see the adapter release notes. For the installation steps, see Chapter 3, “Installing,” on page 11.

Upgrading the adapter profile

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

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

Chapter 5. Configuring

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

Use these options to configure the IBM i Adapter.

- "Customizing the adapter profile" on page 21
- "Specifying the format for date, date separator, and time separator" on page 22
- "Editing adapter profiles on the UNIX or Linux operating system" on page 23

See the *IBM Security Dispatcher Installation and Configuration Guide* for additional configuration options such as:

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

Customizing the adapter profile

To customize the adapter profile, you must modify the IBM i Adapter JAR file, `IDIOS400profile.jar`. You might customize the adapter profile to change the account form or the service form.

About this task

The `IDIOS400profile.jar` file is included in the IBM i Adapter compressed file that you downloaded from the IBM website. The JAR file contains the following files:

Note: You cannot modify the schema for this adapter. Attributes cannot be added to or deleted from the schema.

- CustomLabels.properties
- er IDIOS400Account.xml
- er IDIOS400RMIService.xml
- service.def
- schema.dsml
- IDIOS400AL.xml
- IDIOS400Add.xml
- IDIOS400Delete.xml
- IDIOS400Modify.xml
- IDIOS400Search.xml
- IDIOS400Test.xml

Procedure

1. Log on to the workstation where the IBM i Adapter is installed.
2. Copy the JAR file into a temporary directory.

3. Extract the contents of the JAR file into the temporary directory by running the following command. The following example applies to the IBM i Adapter profile. Type the name of the JAR file for your operating system. The jar command extracts the files into the IDIOS400profile directory.

```
#cd /tmp
#jar -xvf IDIOS400profile.jar
```

4. Edit the file that you want to change. After you edit the file, you must import the file into the Identity server for the changes to take effect.
5. Import the file.
   a) Create a JAR file by using the files in the `/tmp` directory by running the following commands:

```
#cd /tmp
jar -cvf IDIOS400profile.jar IDIOS400profile
```

   b) Import the JAR file into the IBM Security Verify Identity application server.
   c) Stop and start the Identity server
   d) Restart the adapter service.

Related concepts

Password management when restoring accounts
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account. However, in some cases you might not want to supply a new password.

Related tasks

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Specifying the format for date, date separator, and time separator

You can specify how you want to have the time and date displayed by the adapter.

About this task

The IBM i supports the following format for date, date separator, and time separator:

- Date format = YMD, MDY, DMY, and julian
- Date separator = / , . -
- Time separator = : ,

The adapter uses the following formats as default format:

- Date format = YMD
- Date separator = /
- Time separator = :

If the format used by the adapter and the resource format is the same, then customization is not required. However, if the format is different, you can customize the service profile.

Note: The adapter does not support the Julian date format.

Procedure

1. Log on to IBM Security Verify Identity as an administrator.
2. In the My Work pane, expand **Configure System** and click **Design Forms** to display the Design Forms page.
3. From the applet, double-click **Service** to display the service form profiles.
4. Double-click the service form profile that has the service form you want to customize.

5. From the Attributes List window, double-click the **eros400dateformat**, **eros400dateseparatorattribute**, **eros400timeseparator** to add it to the service form.
6. Click **Save Form Template** icon.

Related tasks

Editing adapter profiles on the UNIX or Linux operating system
The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

Editing adapter profiles on the UNIX or Linux operating system

The adapter profile `.jar` file might contain ASCII files that are created by using the MS-DOS ASCII format.

About this task

If you edit an MS-DOS ASCII file on the UNIX operating system, you might see a character `^M` at the end of each line. These characters indicate new lines of text in MS-DOS. The characters can interfere with the running of the file on UNIX or Linux systems. You can use tools, such as **dos2unix**, to remove the `^M` characters. You can also use text editors, such as the **vi** editor, to remove the characters manually.

Example

You can use the **vi** editor to remove the `^M` characters. From the **vi** command mode, run the following command and press Enter:

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

When you use this command, enter `^M` or `Ctrl-M` by pressing **^v^M** or **Ctrl V Ctrl M** sequentially. The **^v** instructs the **vi** editor to use the next keystroke instead of issuing it as a command.

Related tasks

Specifying the format for date, date separator, and time separator
You can specify how you want to have the time and date displayed by the adapter.

Password management when restoring accounts

When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account. However, in some cases you might not want to supply a new password.

When IBM Security Directory Server is used to restore accounts, you are always prompted to enter the new password. But when Sun Java System Directory Server is used to restore an account, you are not required to enter a new password. For IBM i Adapter, the password requirement to restore an account on the directory server 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 Identity to forego the new password requirement. You can set the IBM i Adapter to require a new password when the account is restored, if your company has a business process in place that dictates that the account restoration process must be accompanied by resetting the password.

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

Edit the service.def file to add the new protocol options, for example:

```
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_REQUIRED_ON_RESTORE"><value>true</value>
</property>
<Property Name  = "com.ibm.itim.remoteservices.ResourceProperties.
                  PASSWORD_NOT_ALLOWED_ON_RESTORE"><value>false</value>
</property>
```

By adding the two options in the example above, you are ensuring that you are not prompted for a password when an account is restored.

Note: Before you set the property `password_not_required_on_restore` to `true`, ensure that the operating system supports restoring of an account without a password.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the IBM i Adapter JAR file, `IDIOS400profile.jar`. You might customize the adapter profile to change the account form or the service form.

Verifying that the adapter is working correctly
After you install and configure the adapter, verify that the installation and configuration are correct.

Configuring certificates for one-way SSL authentication

For secure communications, you must configure certificates for one-way SSL communication between IBM Security Directory Integrator and the IBM i Directory Server

About this task

You must configure the certificates for each iSeries system on which you want to use secure connectivity.

Note: The following steps apply to the IBM i V6R1 Digital Certificate Manager web page. If you are using the IBM i V7R1 Digital Certificate Manager web page, the navigation might be different, but the concept is the same.

Procedure

1. Sign on to the iSeries Digital Certificate Manager web page.
   a) Log on to the iSeries Tasks menu.
      Using a browser, enter:

      ```
      http://YouriSeriesServer:2001
      ```

      If the web page is not displayed, type the following command on the IBM i command line:

      ```
      STRTCPSVR *HTTP HTTPSVR(*ADMIN)
      ```

   b) Authenticate with an IBM i user ID and password.

      Note: The user profile must have *ALLOBJ and *SECADM special authorities.

   c) Click **Digital Certificate Manager**.
2. Create a certificate authority (CA).
   a) In the left menu of the Digital Certificate Manager, click **Create a Certificate Authority (CA)**.
   b) Complete the form.

      Certificate store password
      Specifies your certificate password. Record this important information in a secure location for later use.

      Certificate Authority (CA) name
      Specifies the specific system. For example, `irvas01.irvine.ibm.com`.

Note: If you need assistance with any of the other fields, click the help icon (?) in the upper right corner of the display.

c) Click **Continue**.

Note: Do not install the certificate now.

d) Click **Cancel** to exit the menu.

e) In the left menu of the Digital Certificate Manager, click **Install Local CA certificate on your PC**.

f) Select **Copy and paste certificate**. A Base 64 encoded ASCII certificate file is displayed.

g) Copy all the text from 'begin certificate' to 'end certificate'. Paste it to a text file on the workstation that is running the Security Directory Integrator dispatcher service.

h) Click **OK**.

3. Create a *SYSTEM certificate store (database).
   a) In the left menu of the Digital Certificate Manager, click **Create New Certificate Store**.
   b) Select **Other System Certificate Store** and click **Continue**.
   c) Select option **No – Do not create certificates in the store**.
   d) In the **Certificate store path and filename** field, enter the path and file name that you want to use for the new certificate store.
   e) Type the Certificate store password. Record this important information in a secure location for later use.
   f) Click **Continue**. The left pane of DCM is refreshed and the *SYSTEM store is created.
   g) Click **OK**.
   h) Click **Cancel** to exit out of the menu.
4. Define a CA trust list.
   a) Click **Select Certificate Store**.
   b) Select ***SYSTEM** and click **Continue**.
   c) Type the certificate store password and click **Continue**. The screen is refreshed.
   d) Click **Manager Applications** on the left menu.
   e) Select **Define CA Trust List** and click **Continue**.
      i) Select **Server** and click **Continue**.
      ii) Select **IBM Directory Server** and click **Define CA Trust List**.
      iii) Check the **LOCAL_CERTIFICATE_AUTHORITY** check box.
      iv) Click **OK**.

   Repeat steps 4b through 4e for **IBM Directory Sever Publishing** and **IBM Directory Server Client**, but select Client for step 4e1.
5. Create a CA Certificate in the *SYSTEM store.
   a) In the left menu of the Digital Certificate Manager click **Create Certificate**.
   b) Select **Server or client certificate** and click **Continue**.
   c) Select **Local Certificate Authority (CA)** and click **Continue**.
   d) Fill out the form.

   Note: If you need assistance with any of the other fields, click the help icon (?) in the upper right corner of the display.

   e) Click **Continue**.
6. Associate applications with the CA certificate created in the previous step.
   a) Ensure that the components are marked to trust the CA certificate that was created in the previous step.
      - Security Directory Server

- Security Directory Server publishing
- Security Directory Server client

b) Click **Continue**.

c) Click **OK**.

d) Click **Cancel** to exit the menu.

e) Restart the Directory Server.

i) At the command prompt type: `ENDTCPSVR *DIRSRV` and press Enter.

ii) Wait for the service to end.

iii) At the command prompt type: `STRTCPSVR *DIRSRV` and press Enter.

7. Add CA to signer certificates on the workstation where the Security Directory Integrator is installed.

a) Start the **iKeyman** utility. In the *ITDI_HOME_DIR*`\_jvm\jre\bin` directory issue the command **ikeyman.exe**.

b) Create a `.jks` keystore.

c) Select **Signer Certificates**.

d) Click **Add**.

e) Specify the path of the file where IBM i local CA was saved. See step 2 g.

f) Type a description for the file.

g) Exit the **iKeyman** utility.

8. Edit the global.properties and the solution.properties files on the workstation where the Security Directory Integrator is installed.

a) Depending on whether a solutions directory is set up for the Security Directory Integrator, open one or both of these files in a flat editor such as Notepad.

- *ITID_HOME_DIR*\global.properties
- *ITDI_SOL_DIR*\solution.properties

b) Edit the server authentication section.

For example:

```
javax.net.ssl.trustStore=C:\itdicertkeys\iseries.jks
javax.net.ssl.trustStorePassword=fred2134
javax.net.ssl.trustStoreType=jks
```

c) Repeat the same steps for the client authentication section.

d) Restart the dispatcher service.

9. Modify the IBM i service:

a) Adjust the **URL** to use the LDAP SSL port. For example: `ldap://irvas01.irvine.ibm.com:636`.

b) Ensure that the **Use SSL** check box is selected.

c) Verify that you typed the password.

d) Click **Test Connection** at the bottom of the page.

Verifying that the adapter is working correctly

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

Procedure

1. Test the connection for the service that you created on the Identity server.
2. Run a full reconciliation from the Identity server.
3. Run all supported operations such as add, modify, and delete on one user account.

4. Verify the `ibmdi.log` file after each operation to ensure that no errors are reported.
5. Verify the `trace.log` file to ensure that no errors are reported when you run an adapter operation.

Related concepts

Password management when restoring accounts
When an account is restored from being previously suspended, you are prompted to supply a new password for the reinstated account. However, in some cases you might not want to supply a new password.

Related tasks

Customizing the adapter profile
To customize the adapter profile, you must modify the IBM i Adapter JAR file, `IDIOS400profile.jar`. You might customize the adapter profile to change the account form or the service form.

Chapter 6. Troubleshooting

Troubleshooting is a systematic approach to solving a problem. The goal of troubleshooting is to determine why something does not work as expected and how to resolve the problem. This topic provides information and techniques for identifying and resolving problems that are related to the adapter, including troubleshooting errors that might occur during the adapter installation.

Techniques for troubleshooting problems

Certain common techniques can help with the task of troubleshooting. The first step in the troubleshooting process is to describe the problem completely.

Problem descriptions help you and the IBM technical-support representative find the cause of the problem. This step includes asking yourself basic questions:

- What are the symptoms of the problem?
- Where does the problem occur?
- When does the problem occur?
- Under which conditions does the problem occur?
- Can the problem be reproduced?

The answers to these questions typically lead to a good description of the problem, which can then lead you to a problem resolution.

What are the symptoms of the problem?

When you start to describe a problem, the most obvious question is "What is the problem?" This question might seem straightforward; however, you can break it down into several more-focused questions that create a more descriptive picture of the problem. These questions can include:

- Who, or what, is reporting the problem?
- What are the error codes and messages?
- How does the system fail? For example, is it a loop, hang, crash, performance degradation, or incorrect result?

Where does the problem occur?

Determining where the problem originates is not always easy, but it is one of the most important steps in resolving a problem. Many layers of technology can exist between the reporting and failing components. Networks, disks, and drivers are only a few of the components to consider when you are investigating problems.

The following questions help you to focus on where the problem occurs to isolate the problem layer:

- Is the problem specific to one operating system, or is it common across multiple operating systems?
- Is the current environment and configuration supported?
- Do all users have the problem?
- (For multi-site installations.) Do all sites have the problem?

If one layer reports the problem, the problem does not necessarily originate in that layer. Part of identifying where a problem originates is understanding the environment in which it exists. Take some time to completely describe the problem environment, including the operating system and version, all corresponding software and versions, and hardware information. Confirm that you are running within an environment that is a supported configuration. Many problems can be traced back to incompatible levels of software that are not intended to run together or are not fully tested together.

When does the problem occur?

Develop a detailed timeline of events that lead up to a failure, especially for those cases that are one-time occurrences. You can most easily develop a timeline by working backward: Start at the time an error was reported (as precisely as possible, even down to the millisecond), and work backward through the available logs and information. Typically, you use the first suspicious event that you find in a diagnostic log.

To develop a detailed timeline of events, answer these questions:

- Does the problem happen only at a certain time of day or night?
- How often does the problem happen?
- What sequence of events leads up to the time that the problem is reported?
- Does the problem happen after an environment change, such as upgrading or installing software or hardware?

Responding to these types of questions can give you a frame of reference in which to investigate the problem.

Under which conditions does the problem occur?

Knowing which systems and applications are running at the time that a problem occurs is an important part of troubleshooting. These questions about your environment can help you to identify the root cause of the problem:

- Does the problem always occur when the same task is being done?
- Is a certain sequence of events required for the problem to occur?
- Do any other applications fail at the same time?

Answering these types of questions can help you explain the environment in which the problem occurs and correlate any dependencies. Remember that just because multiple problems might occur around the same time, the problems are not necessarily related.

Can the problem be reproduced?

From a troubleshooting standpoint, the ideal problem is one that can be reproduced. Typically, when a problem can be reproduced you have a larger set of tools or procedures at your disposal to help you investigate. Problems that you can reproduce are often easier to debug and solve.

However, problems that you can reproduce can have a disadvantage: If the problem is of significant business impact, you do not want it to recur. If possible, re-create the problem in a test or development environment, which typically offers you more flexibility and control during your investigation.

- Can the problem be re-created on a test system?
- Do multiple users or applications have the same type of problem?
- Can the problem be re-created by running a single command, a set of commands, or a particular application?

Error messages and problem solving

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

Table 3 on page 31 contains warnings or errors which might be displayed in the user interface.

Table 3. Warning and error messages

Warning or error message	Corrective action
No login or an invalid credential was supplied in the request.	The adapter cannot bind to a naming context or is unable to initialize because invalid credentials were provided. To fix this problem, ensure that: • The managed resource is functioning properly and that you are connected to the correct resource. • The naming context is correct if the naming context is customized. • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct.
An error occurred while establishing communication with the IBM Security Directory Integrator server.	IBM Security Verify Identity cannot establish a connection with Security Directory Integrator server. To fix this problem, ensure that: • The Security Directory Integrator server is running • The URL specified on the service form for the Security Directory Integrator server is correct.
Insufficient 'add' privilege.	The administrator ID that is specified on the service form does not have privileges to add a user under the base DN. You must change the administrator ID to an administrator ID that has the correct privileges or assign privileges for the specified administrator ID.
User Already Exists or exception:javax.naming.NameAlreadyBoundException.	The user has already been added to the resource. This error might occur if you are attempting to add a user to the directory server and IBM Security Verify Identity is not synchronized with the resource. To fix this problem, schedule a reconciliation between IBM Security Verify Identity and the resource. See the online help for information about scheduling a reconciliation.
Unknown Error while adding user on resource.	This error might occur for several reasons. To fix this problem, ensure that: • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct. • The base point is correct, if it is customized. • The administrator ID has the correct privileges to modify a user account under the base DN. • The network connection is not slow.
Cannot add user to specific group.	If you cannot add a user to a group, ensure that the specified group was created on the resource.

Table 3. Warning and error messages (continued)

Warning or error message	Corrective action
User not found.	This error might occur when you attempt to add, modify, delete, or search for a user. This error might also occur if you attempt to change the password for a user. To fix the problem, ensure that: • The server that is specified for the adapter is correct. • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct. • The base point is correct, if it is customized. If the error continues to occur, check to ensure that • The user was created on the directory server. • The user was not moved or deleted from the directory server. To fix the problem, add the user to the directory server and then schedule a reconciliation. See the online help for information about scheduling a reconciliation.
Unknown error while modifying user on resource.	This error might occur for several reasons. To fix this problem, ensure that: • The administrator ID specified on the service form is correct. • The administrator password specified on the service form is correct. • The base point is correct, if it is customized. • The administrator ID has the correct privileges to modify a user account under the base DN. • The network connection is not slow.
Error adding user to group.	If you cannot add a user to a group, ensure that • The user was created on the resource. • The user is not already a member of the group. • The group was created on the resource. If the user does not exist on the resource, you must create the user. If a user is already a member of a group, you cannot add the user to the group. If the group does not exist on the resource, you must add the group to the resource before you can add a user to the group. See the online help for information about creating groups or adding users to groups.
Insufficient 'delete' privilege.	The administrator ID that is specified on the service form does not have privileges to delete a user under the base DN. You must change the administrator ID to an administrator ID that has the correct privileges or assign privileges for the specified administrator ID.

Table 3. Warning and error messages (continued)

Warning or error message	Corrective action
Search failed.	This error might occur for several reasons. To fix the problem, ensure that: • The network connection is not slow. • The resource is not overloaded with network traffic. • The Security Directory Integrator server has sufficient memory, if you have a large number of users and groups.

Chapter 7. Uninstalling

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

Deleting the adapter profile

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

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

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

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

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

Chapter 8. Reference

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

Adapter attributes

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

The combination of attributes depends on the type of action that the Identity server requests from the IBM i Adapter. The following table lists the attributes that are used by the IBM i Adapter.

Table 4. Account Attributes, descriptions and permissions

Attribute	Description	Permissions
erOS400AcctgCode	Specifies the accounting code.	Read and Write
erOS400AsstLevel	Specifies the assistance level.	Read and Write
erOS400AttnPgm	Specifies the attention program.	Read and Write
erOS400AuditLevel	Specifies the level of auditing.	Read
erOS400Aut	Specifies the type of authority.	Read and Write
erOS400CharIdCtrl	Specifies the character identifier control for the job.	Read and Write
erOS400CntryID	Specifies the country identifier.	Read and Write
erOS400CodedCharSetID	Specifies the coded character set identifier.	Read and Write
erOS400Curlib	Specifies the current library.	Read and Write
erOS400Delivery	Specifies the delivery type.	Read and Write
erOS400DispSgnOnData	Specifies to display the sign-on data at logon.	Read and Write
erOS400DocPwd	Specifies the document password.	Read and Write
erOS400Eimassoc	Specifies the user profile attribute specifically designed to aid in configuring Enterprise Identity Mapping (EIM).	Read
erOS400GroupAuth	Specifies the group authority.	Read and Write
erOS400GroupAuthType	Specifies the type of group authority.	Read and Write
erOS400GroupID	Specifies the group ID.	Read
erOS400GroupMembers	Displays the members of this group.	Read
erOS400GroupName	Specifies the name of the group.	Read
erOS400GroupProfile	Specifies the profile of the group.	Read and Write

Table 4. Account Attributes, descriptions and permissions (continued)		
Attribute	**Description**	**Permissions**
erOS400HomeDir	Specifies the home directory.	Read and Write
erOS400IaspStorageInfo	Specifies the Iasp storage information.	Read
erOS400IaspStorageUsed	Specifies the amount of Iasp storage used.	Read
erOS400InitialMenu	Specifies the initial menu.	Read and Write
erOS400InitialPgm	Specifies the initial program.	Read and Write
erOS400JobDesc	Specifies the job description.	Read and Write
erOS400KeybrdBuff	Specifies to use keyboard buffering.	Read and Write
erOS400LangID	Specifies the language to use.	Read and Write
erOS400LimitCapabilities	Specifies to limit capabilities.	Read and Write
erOS400LimitDeviceSessions	Specifies to limit the number of device sessions.	Read and Write
erOS400Locale	Specifies the locale.	Read and Write
erOS400LocalPwdMgmt	Specifies to enable local password management.	Read
erOS400MaxStorage	Specifies the maximum amount of storage.	Red and Write
erOS400MessageQ	Specifies the message queue.	Read and Write
erOS400NumInvalidSignOn	Specifies the number of invalid signons.	Read
erOS400ObjAuditing	Specifies to enable object auditing.	Read
erOS400OutQ	Specifies the output queue.	Read and Write
erOS400Owner	Specifies the owner.	Read and Write
erOS400PrintDevice	Specifies the print device.	Read and Write
erOS400PriorityLimit	Specifies the priority limit.	Read and Write
erOS400PwdExpDate	Specifies the date that the password expires.	Read
erOS400PwdExpired	Specifies whether the password is expired.	Read and Write
erOS400PwdExpiredInterval	Specifies the time before a password expires.	Read and Write
erOS400PwdLastChanged	Specifies when the password was last changed.	Read
erOS400SetJobAttr	Specifies the job attributes to be taken from the locale.	Read and Write
erOS400SevCodeFilter	Specifies the severity code filter.	Read and Write

Table 4. Account Attributes, descriptions and permissions (continued)

Attribute	Description	Permissions
erOS400SortSeq	Specifies the sort sequence	Read and Write
erOS400SpecialAuth	Specifies whether special authority is granted.	Read and Write
erOS400SpecialEnv	Specifies special environment.	Read and Write
erOS400StorageCurrUsed	Specifies the storage currently being used.	Read
erOS400SuppGroupProfile	Specifies the supplementary group profile.	Read and Write
erOS400Text	Specifies a description of the profile.	Read and Write
erOS400UID	Specifies the UID.	Read and Write
erOS400UserClass	Specifies the user class.	Read and Write
erOS400UserOptions	Specifies any user options.	Read and Write
erAccountStatus	Specifies whether the account is enabled or disabled.	Read and Write
erPassword	Specifies the password.	Read and Write
Eruid	Specifies the login name and user name.	Read and Write

Table 5. Group Attributes, descriptions and permissions

Attribute	Description	Permissions
erOS400GroupName	Specifies the group name.	Read
erPassword	Specifies the password.	Read
erOS400GroupID	Specifies the group identifier.	Read
erOS400Text	Specifies the description of a group profile.	Read

Index

U

V

W