Oracle® Identity Manager

Connector Guide for IBM OS/400 Advanced

Release 9.0.4

E10452-04

July 2009

ORACLE®

Oracle Identity Manager Connector Guide for IBM OS/400 Advanced, Release 9.0.4

E10452-04

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

Preface

This guide provides information about integrating Oracle Identity Manager with IBM OS/400.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at http://www.oracle.com/accessibility/.

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

Related Documents

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network.

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see Oracle Identity Manager Connector Concepts.

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

`http://www.oracle.com/technology/documentation/index.html`

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack documentation library, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in the Oracle Identity Manager Connector for IBM OS/400?

This chapter provides an overview of the updates made to the software and documentation for the Oracle Identity Manager Connector for IBM OS/400 in release 9.0.4.4.

> **See Also:** The earlier release of this guide for information about updates that were new for that release

The updates discussed in this chapter are divided into the following categories:

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following software updates have been made in releases 9.0.4.1 through 9.0.4.4:

- IBM OS/400 user profile commands supported by the Provisioning Agent have been added in "Functionality Supported by the Provisioning Agent" on page 1-6.
- The list of functions supported by the Provisioning Agent has been updated in "Functionality Supported for Provisioning" on page 1-6.
- The commands supported by the Reconciliation Agent have been updated in "Functionality Supported by the Reconciliation Agent" on page 1-6.
- The list of functions supported by the Reconciliation Agent has been updated in "Functionality Supported for Reconciliation" on page 1-6.
- The list of fields reconciled between Oracle Identity Manager and IBM OS/400 has been updated in "Target System Fields Used for Reconciliation and Provisioning" on page 1-7.
- The IT resource parameters and their corresponding descriptions and sample values have been updated in "Importing the Connector XML File" on page 2-6.

- The procedure to configure the connector for multiple installations of the target system has been added in "Configuring the Connector for Multiple Installations of the Target System" on page 2-11.
- Information about reconciliation based on user status has been added in "Configuring Account Status Reconciliation" on page 4-4.
- Known issues related to the following bugs have been added in Chapter 6, "Known Issues":
  - Bug 7189194
  - Bug 7353425

Documentation-Specific Updates

The following documentation-specific updates have been made in releases 9.0.4.1 through 9.0.4.4:

- The "Verifying Deployment Requirements" section on page 3-1 has been updated with specific IBM OS/400 versions that can be used to deploy the Oracle Identity Manager IBM OS/400 Advanced connector.
- The user profile field mappings between Oracle Identity Manager and the target system have been added in "Target System Fields Used for Reconciliation and Provisioning" on page 1-7. "Appendix A: Attribute Mapping Between Oracle Identity Manager and IBM i5/OS" has been removed.
- The components of the IBM OS/400 Advanced connector and the connector architecture for reconciliation and provisioning have been added in "Connector Architecture" on page 1-2. "Appendix B: Connector Architecture" has been removed.
- Guidelines that were earlier documented in Chapter 6, "Known Issues" have been moved to "Guidelines on Using the Connector" on page 5-1.
- In "Certified Languages" on page 1-2, Arabic has been added to the list of languages that the connector supports.
- In "Certified Deployment Configurations" on page 1-1, changes have been made in the "Target System" row. Information about certified deployment configurations has been removed from "Verifying Deployment Requirements" on page 3-1.

1

About the Connector

The Oracle Identity Manager IBM OS/400 Advanced connector provides a native interface between Oracle Identity Manager and IBM OS/400 installed on the z/OS mainframe. The connector functions as a trusted virtual administrator on the target system, performing tasks such as creating login IDs and changing passwords. In addition, it automates some of the functions that administrators usually perform manually.

The connector enables provisioning and reconciliation with IBM OS/400. This guide discusses the connector that enables you to use IBM OS/400 either as a managed (target) resource or as an authoritative (trusted) source of user data for Oracle Identity Manager.

This chapter discusses the following topics:

- Certified Deployment Configurations
- Certified Languages
- Features of the Connector
- Roadmap for Deploying and Using the Connector

Note: In earlier releases, IBM OS/400 was known as IBM AS/400 or IBM i5/OS. Because the connector development started before the change in nomenclature was formally announced by IBM, the IBM OS/400 connector code, scripts, and nomenclature in the connector pack may have occurrences of AS/400 or i5/OS. These instances are not errors in the documentation.

1.1 Certified Deployment Configurations

Table 1–1 lists the certified deployment configurations.

Table 1–1 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target System	IBM i5/OS and OS/400 releases V5R2, V5R3, V5R4, V6R1
Infrastructure Requirements: message transport layer	JTOpen versions 5.1.1 and 5.2 (open source or commercially supported version)
Target system user account for Oracle Identity Manager	OS/400-authorized account with SystemAdministrators privileges

Note: The LDAP Gateway uses the target system user account that you create for Oracle Identity Manager. Therefore, it has the privileges required to access and operate with the Reconciliation Agent and Provisioning Agent. See "Connector Architecture" on page 1-2 for information about the Reconciliation Agent and Provisioning Agent.

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

1.3 Features of the Connector

This section discusses the following topics:

1.3.1 Connector Architecture

The connector consists of the following components:

- **LDAP Gateway:** The LDAP Gateway is built on Java 1.4 and allows portability among different platforms and operating systems. The LDAP Gateway receives LDAP protocol commands from distributed applications and translates them to native IBM OS/400 commands. After the commands are run, LDAP-formatted responses are returned to the requesting application. It is recommended that you install the LDAP Gateway on the same computer as Oracle Identity Manager.
- **JTOpen Provisioning Agent:** The connector provides the provisioning functionality through the JTOpen Provisioning Agent, which is an IBM OS/400

component. JTOpen receives IBM OS/400 identity and authorization change events from the LDAP Gateway. These events are processed against the IBM OS/400 authentication repository, in which all provisioning updates from the LDAP Gateway are stored. The response is parsed and returned to the LDAP Gateway.

- **Voyager Reconciliation Agent:** The connector provides the reconciliation functionality through the Voyager Reconciliation Agent, which is an IBM OS/400 component. The Reconciliation Agent receives IBM OS/400 identity and authorization change events by using exit technology. Exits are programs that are run after an event in IBM OS/400 is processed. The exits then send the change events in real time to the Reconciliation Agent. These events include events occurring from the command prompt, batch jobs, and other native IBM OS/400 events. The Reconciliation Agent transforms these events into notification messages for Oracle Identity Manager through the LDAP Gateway.
- **Message Transport Layer:** The message transport layer enables the exchange of messages between the LDAP Gateway and the Reconciliation Agent and Provisioning Agent. JTOpen is used as the messaging protocol for the message transport layer. JTOpen is a library of Java classes that lets you implement the client-server and internet programming model with an IBM OS/400 system. The JTOpen classes can be used by Java applets, servlets, and applications to access data and resources on an IBM OS/400 system. JTOpen requires only the Java Virtual Machine (JVM) and the Java Developer Kit (JDK).

  See Also:

  - JTOpen Web site at the following URL for information about the JTOpen project:

    `http://jt400.sourceforge.net/`

  - IBM Toolbox for Java documentation at the following URL for information about the JTOpen functionality:

    `http://www-03.ibm.com/servers/eserver/iseries/toolbox/overview.html`

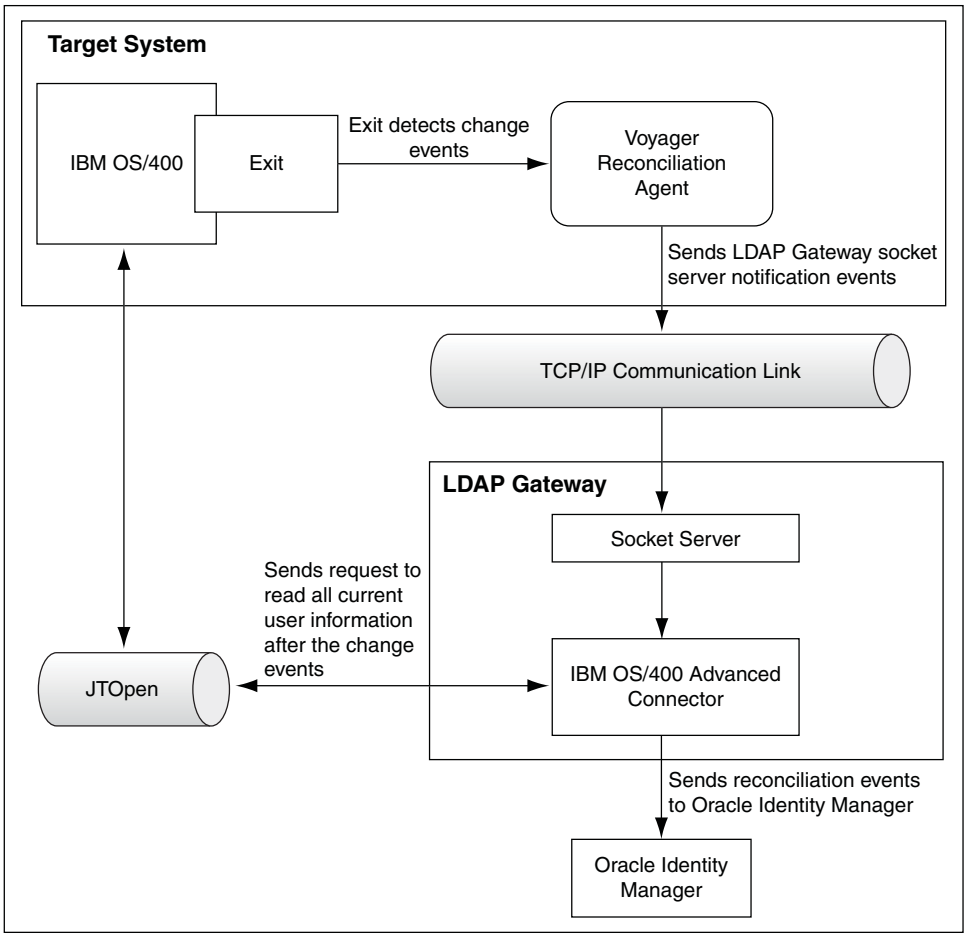
The architecture of the connector can be explained in terms of the connector operations it supports:

- Reconciliation
- Provisioning

1.3.1.1 Reconciliation

Figure 1–1 shows the flow of data during reconciliation:

Figure 1–1 Reconciliation



Reconciliation involves the following steps:

1. IBM OS/400 identity and authorization events take place in the target system. These events are processed through appropriate exits. After processing the events, the exits send them to the Voyager Reconciliation Agent.

   Note: Identity and authorization events in the IBM OS/400 system include the running of a command, real-time password synchronization, creation or deletion of a user, or a change in the user data.

2. The Reconciliation Agent transforms these events into notification events or messages for the LDAP Gateway. The notification messages consist of encrypted files. The Reconciliation Agent opens a new socket to the LDAP Gateway and sends the encrypted notification messages. The messages are sent to the LDAP Gateway through the message transport layer. These messages contain the minimum amount of data required to reconcile the event, such as the message type, user id, and password (for a password change event).
3. The LDAP Gateway receives the messages from the Reconciliation Agent and decrypts them for the connector.

4. The connector sends a request to the JTOpen Provisioning Agent to retrieve all the current user data that is generated as a result of the IBM OS/400 identity and authorization events.

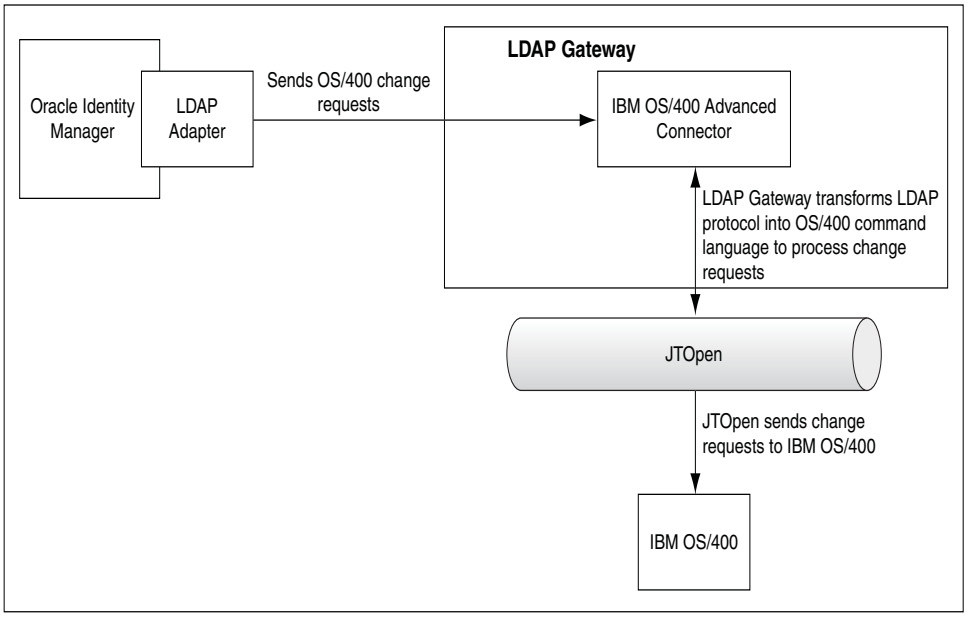
> **Note:** JTOpen acts uses TCP/IP to send IBM OS/400 commands. JTOpen acts as the message transport layer as well as the provisioning agent. See "Provisioning" on page 1-5 for more information about JTOpen as the provisioning agent.

5. If an event fetched from the target system matches with the notification data, then the connector returns an error and the process stops. If the event does not match, then the connector sends the event to Oracle Identity Manager for reconciliation and updates the internal meta-store of event records. This process is repeated for all the events that are fetched from the target system.

1.3.1.2 Provisioning

Figure 1–2 shows the flow of data during provisioning:

Figure 1–2 Provisioning



Provisioning involves the following steps:

1. A user is created, updated, or deleted in Oracle Identity Manager.
2. The Oracle Identity Manager process task adapter for IBM OS/400 forwards the change request to the LDAP Gateway.
3. The LDAP Gateway translates the change requests to IBM OS/400 commands. The IBM OS/400 Advanced connector encrypts the data, and sends it to the JTOpen Provisioning Agent, which also functions as the message transport layer.
4. The connector also updates the internal meta-store of the LDAP Gateway with the changes in user data.
5. JTOpen decrypts the data, sends the data to the IBM OS/400 repository, and returns success or error messages back to the LDAP Gateway.

Note: No agents are required on the target system to support the provisioning capabilities of the connector. Provisioning is achieved by using a network-aware API located on the Oracle Identity Manager host computer. Reconciliation requires an agent on the target system to detect changes and also uses the network-aware API.

1.3.2 Functionality Supported by the Reconciliation Agent

The Voyager Reconciliation Agent supports reconciliation of changes that are made to user profiles by using commands such as CRTUSRPRF or CHGUSRPRF. These commands also contain users' passwords for reconciliation, if any.

1.3.3 Functionality Supported for Reconciliation

The Reconciliation Agent supports the following functions:

- Create user data event
- Modify user data event
- Delete user event
- Password change event
- Disable user event
- Enable user event

1.3.4 Functionality Supported by the Provisioning Agent

The Provisioning Agent uses the following IBM OS/400 user profile commands:

- [ADDUSER]: Creates an IBM OS/400 user profile
- [CHGUSRPRF]: Modifies an existing IBM OS/400 user profile
- [DLT]: Deletes an IBM OS/400 user profile

1.3.5 Functionality Supported for Provisioning

Table 1–2 describes the functions supported by the Provisioning Agent.

Table 1–2 Functionality Supported for Provisioning

Function	Description
Create OS/400 User	Creates a user
Modify OS/400 User	Modifies a user
Delete OS/400 User	Deletes a user
Change OS/400 Password	Changes the password of a user
Reset OS/400 Password	Resets the user password
Revoke OS/400 User Account	Revokes the user account
Resume OS/400 User Account	Resumes a revoked user account

1.3.6 Target System Fields Used for Reconciliation and Provisioning

Table 1–3 lists the target system fields that are used for reconciliation and provisioning operations.

Table 1–3 Field Mapping Between Oracle Identity Manager and IBM OS/400

Oracle Identity Manager Field	IBM OS/400 Field	Description
uid	USER	User login ID
cn	NAME	User full name
sn	NAME	User last name
userPassword	PASSWORD	Password used to login
owner	OWNER	The owner of the user profile
status	STATUS	User status (enable, disable)
specialAuthority	SPECAUTH	Special access permissions for the user
usrcls	USRCLS	Special access control for the user
inlprg	INLPRG	User initial program
text	TEXT	Free form text field
lmtcpb	LMTCPB	Limit capabilities
jobd	JOBD	Job description
supgrpprf	SUPGRPPRF	Supplemental group
inlmnu	INLMNU	Initial menu
grpprf	GRPPRF	Group profile
passwordExpire	PWDEXP	User password is set to expire

1.4 Roadmap for Deploying and Using the Connector

The IBM OS/400 Advanced connector deployment involves deploying the LDAP Gateway and the Reconciliation Agent. The Reconciliation Agent is deployed on IBM OS/400.

These procedures are described in the following chapters:

- Chapter 2, "Connector Deployment on Oracle Identity Manager" provides instructions for deploying the connector on the Oracle Identity Manager host computer. This procedure involves configuring Oracle Identity Manager, importing the connector XML file, compiling adapters, installing the LDAP Gateway, and configuring the message transport layer.
- Chapter 3, "Connector Deployment on IBM OS/400" describes the procedure to deploy the Reconciliation Agent on IBM OS/400. It is recommended that you perform this procedure with the assistance of the systems programmer.
- Chapter 4, "Configuring the Connector" describes the procedure to run initial reconciliation and to configure trusted source reconciliation and account status reconciliation.
- Chapter 5, "Troubleshooting" states the problem scenarios commonly associated with the connector and the possible solutions to those problems. In addition, this chapter discusses some guidelines on using the connector.

- Chapter 6, "Known Issues" lists the known issues associated with this release of the connector.

2

Connector Deployment on Oracle Identity Manager

The following sections in this chapter describe the procedure to deploy the connector and the LDAP Gateway on the Oracle Identity Manager host computer:

- Files and Directories that Comprise the Connector
- Copying the Connector Files
- Configuring Oracle Identity Manager
- Importing the Connector XML File
- Compiling Adapters
- Configuring the Message Transport Layer
- Installing and Configuring the LDAP Gateway

Refer to the following section if you want to configure the connector for multiple installations of the target system:

- Configuring the Connector for Multiple Installations of the Target System

> **See Also:** Chapter 3, "Connector Deployment on IBM OS/400" for the procedure to deploy the Reconciliation Agent and Provisioning Agent on the target system

2.1 Files and Directories that Comprise the Connector

Table 2–1 lists the contents of the connector installation media.

Table 2–1 Files and Directories That Comprise the Connector

File or Directory on the Installation Media	Description of Files and Contents
etc/LDAP Gateway/ldapgateway.zip	Files required to deploy the LDAP Gateway
etc/Provisioning and Reconciliation Connector/OIMIDFEX.SAVF	Connector agent file to be placed on the target system for deployment on the mid-range system
lib/as400-adv-agent-recon.jar	JAR file containing the files required to enable real-time reconciliation
lib/as400-adv-provisioning.jar	JAR file containing the files required to enable provisioning

Table 2–1 (Cont.) Files and Directories That Comprise the Connector

File or Directory on the Installation Media	Description of Files and Contents
lib/as400Connection.properties	Properties file that specifies the controls for the initial reconciliation run between Oracle Identity Manager and the target system
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Oracle Identity Manager Administrative and User Console.
Files in the scripts directory: ■ scripts/run_initial_recon_provisioning.sh ■ scripts/run_initial_recon_provisioning.bat ■ as400-adv-initial-recon.jar ■ initialAs400Adv.properties	Files that are used to perform first-time (initial) reconciliation with Oracle Identity Manager
scripts/user.txt	Sample of the file containing user data that is used during initial reconciliation See "Running Initial Reconciliation" on page 4-2 for information about using this file.
xml/oimAs400AdvConnector.xml	This XML file contains definitions for the connector components related to reconciliation and provisioning. These components include: ■ Resource objects ■ IT resource types ■ Process forms ■ Process tasks and adapters ■ Provisioning process ■ Lookup definitions ■ Prepopulate rules
xml/AS400TrustedXellerateUser.xml	The XML file that contains component definitions for the connector for trusted source reconciliation

See Also:

- "Copying the Connector Files" on page 2-2
- "Deploying the Reconciliation Agent" on page 3-1

2.2 Copying the Connector Files

Copy the following connector files to the destinations on the Oracle Identity Manager host computer as indicated in Table 2–2.

Note: See "Files and Directories that Comprise the Connector" on page 2-1 for more information about these files. Do not copy the files that are not listed in this table. Those files are used later in the deployment procedure.

Table 2–2 Copying the Connector Files

Files	Destination
etc/LDAP Gateway/ldapgateway.zip	*LDAP_INSTALL_DIR* This is the directory on the Oracle Identity Manager host computer on which you want to install the LDAP Gateway. See "Installing and Configuring the LDAP Gateway" on page 2-9 for information about installing the LDAP Gateway.
lib/as400-adv-agent-recon.jar lib/as400Connection.properties	*LDAP_INSTALL_DIR/etc*
lib/as400-adv-provisioning.jar Files in the scripts directory: ▪ run_initial_recon_provisioning.sh ▪ run_initial_recon_provisioning.bat ▪ as400-adv-initial-recon.jar ▪ user.txt ▪ initialAs400Adv.properties	*OIM_HOME*/JavaTasks/
Files in the resources directory	*OIM_HOME*/connectorResources/
xml/oimAs400AdvConnector.xml xml/AS400TrustedXellerateUser.xml	*OIM_HOME*/XLIntegrations/as400/xml/

While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the files in the connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.

2.3 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

Note: In a clustered environment, you must perform this step on each node of the cluster.

2.3.1 Clearing Content Related to Connector Resource Bundles from the Server Cache

While you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/connectorResources directory. Whenever you add a new resource bundle in the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, go to the *OIM_HOME*/bin directory.

   Note: You must perform step 1 before you perform step 2. An exception is thrown if you run the command described in Step 2 as follows:

   OIM_HOME/bin/*BATCH_FILE_NAME*

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

   In this command, `ConnectorResourceBundle` is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

   OIM_HOME/config/xlConfig.xml

2.3.2 Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- `ALL`

  This level enables logging for all events.

- `DEBUG`

  This level enables logging of information about fine-grained events that are useful for debugging.

- `INFO`

  This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

  This level enables logging of information about error events that may allow the application to continue running.

- FATAL

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- OFF

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines:

     ```
     <category name="COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER">
        <priority value="LOG_LEVEL"/>
     </category>
     ```

  2. In the second XML line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     ```
     <category name="COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER">
        <priority value="INFO"/>
     </category>
     ```

  After you enable logging, log information is written to the following file:

  JBOSS_HOME/server/default/log/server.log

- **IBM WebSphere Application Server:**

  To enable logging:

  1. In the *OIM_HOME*/config/log.properties file, add the following line:

     log4j.logger.COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER=*LOG_LEVEL*

  2. In this line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     log4j.logger.COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER=INFO

  After you enable logging, log information is written to the following file:

  WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/startServer.log

- **BEA WebLogic Server**

  To enable logging:

  1. In the *OIM_HOME*/config/log.properties file, add the following line:

     log4j.logger.COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER=*LOG_LEVEL*

  2. In this line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     log4j.logger.COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER=INFO

  After you enable logging, log information is written to the following file:

  WEBLOGIC_HOME/user_projects/domains/*DOMAIN_NAME*/*SERVER_NAME*/*SERVER_NAME*.log

- **Oracle Application Server**

  To enable logging:

  1. In the *OIM_HOME*/config/log.properties file, add the following line:

     ```
     log4j.logger.COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER=LOG_LEVEL
     ```

  2. In this line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     ```
     log4j.logger.COM.THORTECH.XL.AS400.ADVANCED.UTIL.OIMLOGGER=INFO
     ```

  After you enable logging, log information is written to the following file:

  ```
  OAS_HOME/opmn/logs/default_group~home~default_group~1.log
  ```

2.4 Importing the Connector XML File

To import the connector XML file into Oracle Identity Manager:

1. Open the Administrative and User Console.
2. Click **Deployment Management** on the left navigation pane.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the oimAs400AdvConnector.xml file, which is in the *OIM_HOME*/XLIntegrations/i5OS/xml/ directory. Details of this XML file are shown on the File Preview page.

   You must import the XML file for trusted source reconciliation, AS400TrustedXellerateUser.xml, after the other XML file is imported. In other words, you must import oimAs400AdvConnector.xml regardless of whether you want to implement target resource or trusted source reconciliation. If you want to implement trusted source reconciliation, then import the AS400TrustedXellerateUser.xml file after the first one is imported.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page is displayed.
8. Create an IT resource based on the OIMLDAPGatewayResourceType IT resource type. You must specify values for the IT resource parameters listed in Table 2–3.

Table 2–3 Defining IT Resources

Parameter	Description
AtMap User	Name of the lookup definition containing attribute mappings that are used for provisioning Value: `AtMAp.AS400` **Note:** You must not change the value of this parameter.
idfPrincipalDn	Enter the administrator ID for connecting to the LDAP Gateway Sample value: `cn=idfAs400Admin,dc=as400,dc=com`
idfPrincipalPwd	Enter the administrator password for connecting to the LDAP Gateway
idfRootContext	This parameter holds the root context for IBM OS/400 Value: `dc=as400,dc=com` **Note:** You must not change the value of this parameter.
idfServerHost	This parameter holds the host name for connecting to the LDAP Gateway Value: `localhost` **Note:** You must not change the value of this parameter if you install the LDAP Gateway on the host computer on which Oracle Identity Manager is installed. If you install the LDAP Gateway on a different computer, then specify the host name or IP address of that computer. However, it is recommended that you install the LDAP Gateway on the same computer on which you are installing Oracle Identity Manager.
idfServerPort	Enter the port number for connecting to the LDAP Gateway Sample value: `5389`

9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the OIMLDAPGatewayResourceType IT resource type is displayed.
10. Click **Skip** to indicate that you do not want to define another IT resource. The Confirmation page is displayed.
11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.
12. Click **Import**. The connector file is imported into Oracle Identity Manager.

2.5 Compiling Adapters

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- OnBoardAs400User
- ChangeAs400AdvUserPassword

- ResetAs400AdvPassword
- DeleteAs400AdvUser
- RevokeAs400AdvUser
- ResumeAs400AdvUser
- ModifyAs400AdvUser
- ModifyRemoveAs400AdvUser

You must compile these adapters before they can be used in provisioning operations. To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you have imported into the current database, click **Compile All**.

   If you have created your own adapters or if a new adapter is shipped with a patch that you installed, then you might need to compile one adapter at a time. To compile multiple (but not all) adapters, select the adapters you want to compile. Then, click **Compile Selected**.
3. Click **Start.** Oracle Identity Manager compiles the adapters that you specify.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM_HOME*/adapters/ directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

2.6 Configuring the Message Transport Layer

The connector uses JTOpen as the message transport layer to access OS/400 data and resources from the Oracle Identity Manager host computer. More specifically, it is used by the LDAP Gateway to communicate with the Reconciliation Agent that is installed on the IBM OS/400 system.

> **See Also:** "Connector Architecture" on page 1-2 for more information about JTOpen

To configure JTOpen as the message transport layer:

1. Download JTOpen from the IBM Web site at and unzip the jtopen_ver`.zip` file. You can download JTOpen from the following URL:

   `http://www14.software.ibm.com/webapp/download/search.jsp?go=y&rs=expastbjm3`
2. Copy the jt400.jar and uti400.jar files from the *JTOPEN_INSTALL_DIR*/jtopen/lib/ directory to the *LDAP_INSTALL_DIR*/lib/ directory.

Note:

- The directory on which you install JTOpen is referred to as *JTOPEN_INSTALL_DIR*.
- You must also configure the LDAP Gateway to use JTOpen as the message transport layer. This is covered in "Installing and Configuring the LDAP Gateway" on page 2-9.

2.7 Installing and Configuring the LDAP Gateway

To install and configure the LDAP Gateway:

1. Extract the contents of the ldapgateway.zip file to a directory on the computer on which Oracle Identity Manager is installed.

   Note: In this document, the location (and name) of the ldapgateway directory is referred to as *LDAP_INSTALL_DIR*.

2. Open the *LDAP_INSTALL_DIR*/conf/as400.properties file and specify the values for the parameters of the JTOpen message transport layer, as described in Table 2–4.

Table 2–4 Configuring the LDAP Gateway

Parameter	Sample Value	Description
host	`127.0.0.1`	Target system IP address for the Provisioning Agent host computer
adminId	`test`	Target system administrator ID
adminPwd	`test`	Target system administrator password
agentHost	`127.0.0.1`	Target system IP address for the Reconciliation Agent host computer
agentAdminId	`test`	Target system Reconciliation Agent administrator ID
agentAdminPwd	`test`	Target system Reconciliation Agent administrator password
agentLib	`LSVALGAARD`	Target system library in which the Reconciliation Agent files are located
agentFile	`QCSRC`	Reconciliation Agent file on the target system
agentMember	`EUSRPWD`	Reconciliation Agent user with privileges to retrieve reconciliation event information
agentport	`5490`	Target system port allocated to the Reconciliation Agent
defaultDelete	`delete`	Delete users or revoke access rights during Disable User provisioning operations Set `delete` as the value of this property if you want the user to be deleted from the target system as the outcome of a Delete User provisioning operation. Set `revoke` as the value of this property if you want the user to be disabled on the target system as the outcome of a Delete User provisioning operation.

3. In a text editor, open the following scripts:
   - Open the run.sh or run.bat file from the *LDAP_INSTALL_DIR*/bin/ directory.
   - Open the run_initial_recon_provisioning script file from the *OIM_HOME*/JavaTasks/ directory.
4. In the run script:
   - Set the JAVA_HOME property as follows:

     `JAVA_HOME=`*`DIRECTORY_LOCATION`*`\j2sdj1.4.2_13`

     Replace *`DIRECTORY_LOCATION`* with the full path of the directory.

- If you plan to run multiple LDAP Gateways on a Linux or Solaris environment and there are not enough socket file descriptors to open up all the ports needed for the server, then add the following line:

  ```
  -Djava.nio.channels.spi.SelectorProvider=sun.nio.ch.PollSelectorProvider
  ```

5. In the run and run_initial_recon_provisioning scripts, uncomment the line related to the application server directory. In addition, change the path to reflect the actual location of the application server directory.

   Note: The contents of the run and run_initial_recon_provisioning scripts are similar. You must make the same change in both the scripts.

   The lines starting with a number sign (#) are comments, as shown:

   ```
   ##### SET JBOSS HOME ##################
   #APPSERVER_HOME=/opt/ldapgateway/lib/jboss-4.0.2
   ```

   To uncomment the line, remove the number sign. For example, to ensure that the connector works with JBoss Application Server, change the line to the following:

   ```
   ##### SET JBOSS HOME ##################
   APPSERVER_HOME=/opt/ldapgateway/lib/jboss-4.0.2
   ```

6. If you are using IBM WebSphere Application Server 6.1, then add the com.ibm.ws.wccm_6.1.0.jar file to the CLASSPATH variable in the run and run_initial_recon_provisioning scripts as shown in the following example:

   ```
   rem
   rem SET WEBSPHERE APPLICATION SERVER REQUIRED LIBRARIES
   rem
   set CLASSPATH=%CLASSPATH%;"%APPSERVER_HOME%"\lib\com.ibm.ws.wccm_6.1.0.jar
   ```

7. Open the *LDAP_INSTALL_DIR*/etc/as400Connection.properties file and edit the following property:

   Note: You must also make this change in the initialAs400Adv.properties file, which is in the *OIM_HOME*/JavaTasks directory.

   ```
   _itResource_=NAME_OF_THE_NEW_IT_RESOURCE
   ```

   Replace *NAME_OF_THE_NEW_IT_RESOURCE* with the name of the IT resource that you create by performing Step 8 of the procedure described in "Importing the Connector XML File" on page 2-6.

8. From the *LDAP_INSTALL_DIR*/dist/idfserver.jar file, extract the beans.xml file, open it in an editor, and set values for the following:

   - Target system administrator credentials

     You must change the administrator credentials stored in the following lines of the beans.xml file:

Note: In these lines, the values that you can change are highlighted in bold font. The values that you enter in the beans.xml file must be the same as the values that you specify for the IT resource parameters and the properties in the as400Connection.properties and initialAs400Adv.properties files.

```
<property name="adminUserDN" value="cn=idfAs400Admin,dc=as400,dc=com"/>
<property name="adminUserPassword" value="password"/>
```

- Port used for communication between the LDAP Gateway and the mainframe logical partition (LPAR) that you use for the connector installation

  The default value of the port property is `5389`. If you want to change this value, then edit the value of the port property defined in the beans.xml file:

  ```
  <property name="port" value="5389"/>
  ```

- Configuration for provisioning and initial reconciliation

  If you want the connector to perform provisioning and initial reconciliation but not real-time reconciliation, then change the value from `true` to `false` in the following property:

  ```
  <property name="agent" value="true"/>
  ```

  Do not change the value of the agent property if you want the connector to perform real-time reconciliation.

9. Save the changes made to the beans.xml file, and then re-create the idfserver.jar file.

2.8 Configuring the Connector for Multiple Installations of the Target System

You can configure the connector for multiple installations of the target system. You can also configure the connector for a scenario in which multiple logical partitions (LPARs), which are not associated with the first LPAR, are configured in the target system.

For each installation of the target system, you create an IT resource and configure an additional instance of the LDAP Gateway.

To configure the connector for the second installation of the target system:

Note: Perform the same procedure for each additional installation of the target system.

1. Create an IT resource based on the OIMLDAPGatewayResourceType IT resource type.

   See Also:

   - *Oracle Identity Manager Design Console Guide* for information about creating IT resources
   - Step 8 of "Importing the Connector XML File" on page 2-6 for information about the parameters of the IT resource

2. Copy the current *LDAP_INSTALL_DIR* directory, including all the subdirectories, to a new location.

   Note: In the remaining steps of this procedure, *LDAP_INSTALL_DIR* refers to the newly copied directory.

3. Extract the contents of the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.
4. In the beans.xml file, change the value of the port in the <property name="port" value="xxxx"/> line to specify a port that is different from the port used for the first instance of the LDAP Gateway. The default port number is shown in the following example:

   ```
   <bean id="listener" class="com.identityforge.idfserver.nio.Listener">
   <constructor-arg><ref bean="bus"/></constructor-arg>
   <property name="admin"><value>false</value></property>
   <property name="config"><value>../conf/listener.xml</value></property>
   <property name="port" value="5389"/>
   </bean>
   ```

   If you change the port number, then you must make the same change in the value of the idfServerPort parameter of the IT resource that you create.
5. Save and close the beans.xml file.
6. Open the *LDAP_INSTALL_DIR*/conf/as400.properties file and edit the following properties:
   - _host_=*IP_ADDRESS_OR_HOST_NAME_OF_THE_MAINFRAME*
   - _port_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_PROVISIONING_AGENT*
   - _agentPort_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_RECONCILIATION_AGENT*

   Note: The value of the _agentPort_ property must not be the same as that of the first instance if a second LPAR, which is not associated with the first LPAR, is configured in the target system. This value can be the same as the value of the idfServerPort property if you have two mainframe servers with IBM OS/400 running on each server.
7. Open the *LDAP_INSTALL_DIR*/etc/as400Connection.properties file and edit the following property:

   itResource=*NAME_OF_THE_NEW_IT_RESOURCE*

3

Connector Deployment on IBM OS/400

You must install the Reconciliation Agent component of the connector on the mainframe. The following sections describe the installation and configuration of this agent and of the exits required for this agent:

- Verifying Deployment Requirements
- Deploying the Reconciliation Agent
- Installing the Exits for the Reconciliation Agent
- Configuring the Message Transport Layer

3.1 Verifying Deployment Requirements

Both the Reconciliation Agent and Provisioning Agent need a started task and service account that has the privileges required to run IBM OS/400 system commands on the mainframe.

In addition, these agents function under a user account on the mainframe. This user account must be created by the systems programmer before you deploy the agents.

Note: Both the Provisioning Agent and Reconciliation Agent user accounts require the `SystemAdministrators` group privileges on the OS/400 system.

3.1.1 Environmental Settings and Requirements

The Reconciliation Agent operates by using user exit technology, outside the mainframe operating system. This means that it runs in a different LPAR from the operating system.

A command execution is passed through an exit, just before full completion of the native mainframe command. If the exit fails, then the command fails and returns an error message. Maintaining a specific password format is an example of the objective for which you use custom exits. Oracle Identity Manager exits are engineered to be the last exits called in sequence, which allows the existing exits to function normally. After modifying exits within an LPAR, an initial program load (IPL) of the LPAR may be required.

3.2 Deploying the Reconciliation Agent

You must deploy the Reconciliation Agent on the target system. The Provisioning Agent does not require any special configuration during the connector deployment. To

use the provisioning functionality of this connector, you must ensure that the LDAP Gateway and the message transport layer are configured correctly.

See Also:

- "Installing and Configuring the LDAP Gateway" on page 2-9 for the procedure to install and configure the LDAP Gateway
- "Configuring the Message Transport Layer" on page 3-6 for the procedure to install and configure the message transport layer

To deploy the Reconciliation Agent:

1. Transmit or FTP the /etc/Provisioning and Reconciliation Connector/OIMIDFEX.SAVF file to any directory on the mainframe.

   Note: For this procedure, the directory to which this file is transmitted will be referred to as LSVALGAARD.

2. To view the contents of the OIMIDFEX.SAVF file, run the `DSPSAVF` command as shown:

   ```
   DSPSAVF   FILE(SAMPLIB/OIMIDFEX)
   ```

   The following is the output of the DSPSAVF command:

   ```
   ================================================================================
                         Display Saved Objects - Save File          ,

   Library saved  . . . :   ORIGLIB              Release level  . . . :
   V4R5M0
   ASP  . . . . . . . . :   1                    Data compressed  . . :   No
   Save file  . . . . . :   OIMIDFEX             Objects displayed  . :   3
     Library  . . . . . :     ORIGLIB            Objects saved  . . . :   3
   Records  . . . . . . :   688                  Access paths . . . . :   0
   Save command . . . . :   SAVOBJ
   Save active  . . . . :   *NO
   Save date/time . . . :   01/20/07   01:28:35

   Type options, press Enter.
     5=Display saved data base file members

   Opt  Object             Type     Attribute     Owner         Size (K)   Data
        XUSRPWD            *PGM     CLE           ORIGLIB            236   YES
        NOTIFY             *PGM     CLE           ORIGLIB             68   YES
        QCSRC              *FILE    PF            ORIGLIB             24   YES

   F3=Exit        F12=Cancel

   ================================================================================
   ```

3. Restore the objects in the OIMIDFEX.SAVF file by running the `RSTOBJ` (restore object) command. The following is the syntax for this command:

   ```
   RSTOBJ OBJ(*ALL) SAVLIB(ORIGLIB) DEV(*SAVF) SAVF(SAMPLIB/OIMIDFEX)
   RSTLIB(NEWLIB)
   ```

   The RSTOBJ command saves the restored objects in a new target library. In the command:

- The SAVLIB parameter takes the original library name as input. In the command, replace *ORIGLIB* with the original library name.
- DEV(*SAVF) indicates that a savefile is used.
- The SAVF parameter takes the directory name and file name of the savefile.
- The RSTLIB parameter takes the new library in which you restore the save file objects. In the command, replace *NEWLIB* with the name of the new library.

If required, specify the general public library (QGPL) as the new target library. The QGPL is an existing library on IBM OS/400 that can be used by the system or a user.

3.3 Installing the Exits for the Reconciliation Agent

After copying the connector save file to the LSVALGAARD directory, you install the exits for the Reconciliation Agent. As mentioned earlier, the connector exits are engineered to be the last exits called in sequence, allowing existing exits to function normally. To install the exits for the Reconciliation Agent:

Note: The Reconciliation Agent can be installed using either a menu-driven or a command-driven installation protocol. The following procedure assumes the use of the menu-driven protocol.

---

1. Log in to the IBM OS/400 system as a system administrator.
2. Ensure that the connector library files and objects are present in the LSVALGAARD directory.

   See Also: "Deploying the Reconciliation Agent" on page 3-1 for the procedure to copy the connector files to the LSVALGAARD directory

3. Start the WRKREGINF User Exit Registration program, as shown:

```
Parameters or command
===> WRKREGINF
```

   In IBM OS/400, exit programs are called dynamically. This means that if an exit program is registered with the system, then you can replace the program with a new version, without the need to register the new version.

4. You must register the exit points that are required for the Reconciliation Agent with IBM OS/400. From the menu that is displayed when you run the WRKREGINF program, select option 8 for the exit points that you want to register, either as a group or one at a time. The following exits are registered:

```
QIBM_QSY_CHG_PROFILE  CHGP0100     *YES     Change User Profile
QIBM_QSY_CRT_PROFILE  CRTP0100     *YES     Create User Profile
QIBM_QSY_DLT_PROFILE  DLTP0200     *YES     Delete User Profile - before
QIBM_QSY_RST_PROFILE  RSTP0100     *YES     Restore User Profile
QIBM_QSY_VLD_PASSWRD  VLDP0100     *YES     Validate Password
```

   Each exit point has an exit point format associated with it. The format that is passed to the exit program determines the format of the other information passed to it.

   The CHG_PROFILE (change), CRT_PROFILE (create), and DLT_PROFILE (delete) exit points are used to change, create, and delete user profiles, respectively.

Note: Deleting a user profile can take a long time because a user may own multiple objects, and therefore, be present on many lists and internal tables. After a user is deleted, cleaning up all the entries for the user takes a long time to process. Therefore, you can use a batch job to run the cleanup process. There are two delete points: before the start of the cleanup job and at the end of the cleanup job. This means that in the process of deleting the user profile, there are only two times when actions are monitored. The Reconciliation Agent monitors only the delete point before the cleanup job.

5. Register the following exit points:

   - RST_PROFILE (restore): This is used when user profiles are restored from a save file during a normal operation, and not during the restore operation of the entire system.
   - VLD_PASSWRD : This is called when the password is changed by the user.

     Note: The RST_PROFILE exit point is not called when a user profile is created with the initial password or when the security administrator changes the password for a user. This IBM design limitation has been fixed in IBM OS/400 V5R4 by introducing another exit point called QIBM_QSY_CHK_PASSWRD.

   - XUSRPWD: This must be registered with QIBM_QSY_CHG_PROFILE. However, when you try to register, you might find that there is an existing exit program registered for this point. In the following code snippet, QGLDPUEXIT represents this exit point in the main system library QSYS, which implies that the IBM OS/400 system itself uses this exit point to extend its functionality.

```
                Exit
              Program     Exit
 Opt           Number     Program        Library
 1                        XUSRPWD        LSVALGAARD
          2147483647     QGLDPUEXIT     QSYS
```

     You must also consider the Exit Program Number, which determines the order in which the exit programs run. The system exit program is typically the last to run in the processing order, and therefore, has a very large Exit Program Number (2147483647). Enter the Oracle Identity Manager custom user exit program and the library for it, and select option 1 for adding the exit program.

6. Press the Enter key. The Add screen is displayed with the following values:

```
Exit point . . . . . > QIBM_QSY_CHG_PROFILE
Exit point format  . . . . . > CHGP0100      Name
Program number . . . . . > 1             1-2147483647, *LOW, *HIGH
Program  . . . . . > XUSRPWD       Name
  Library  . . . . . >   LSVALGAARD  Name, *CURLIB
Threadsafe . . . . . .   *UNKNOWN      *UNKNOWN, *NO, *YES
Multithreaded job action . .   *SYSVAL       *SYSVAL, *RUN, *MSG, *NORUN
Text 'description' . . . . .   *BLANK
```

   Press the Enter key to add the program, and then the F5 key to refresh the system to display the result.

Note: An exit program runs in the environment (called an activation group) of the job or user issuing the command to call the exit program. Therefore, the current library (*CURLIB) value changes often and the system might not be able to locate the exit program. The library from which the system can find the exit program is usually hard coded into the exit program registration, as shown in the screen output.

7. Register the exit points as shown in the following screen output:

```
              Program     Exit
 Opt           Number     Program        Library

                    1     XUSRPWD        LSVALGAARD
           2147483647     QGLDPUEXIT     QSYS


Exit point:   QIBM_QSY_CHG_PROFILE     Format:   CHGP0100

Exit point:   QIBM_QSY_CRT_PROFILE     Format:   CRTP0100

Exit point:   QIBM_QSY_DLT_PROFILE     Format:   DLTP0200

Exit point:   QIBM_QSY_RST_PROFILE     Format:   RSTP0100

Exit point:   QIBM_QSY_VLD_PASSWRD     Format:   VLDP0100
```

Note: On IBM OS/400 V5R4, you also register the CHK_PASSWRD exit point.

8. Enter the WRKSYSVAL command and scroll down to the following line:

```
QPWDVLDPGM  *SEC     Password validation program
```

   The WRKSYSVAL command allows you to change the system values that control most of the system configuration.

   Note: Before the General Registration Facility was introduced, a password validation program was used. This was handled through the system value settings.

9. Select option 2 for QPWDVLDPGM.

10. After the XUSRPWD exit program is added to the various exit points, add the NOTIFY exit program to the exit points. The NOTIFY program notifies the LDAP Gateway of a real-time event. This exit program must be defined with Program Number 2, because it must be triggered after the XUSRPWD exit program is run. The NOTIFY exit program must be registered only for the CHGP0100, CRTP0100, and DLTP0200 exits.

This completes the installation of the Reconciliation Agent exits.

Note:

- Do not specify an exit program instead of *REGFAC because this will interfere with an existing validation program. This method of specifying a validation program is no longer valid. The IBM OS/400 Advanced connector code does not support the obsolete validation program.
- The QSECURITY system value determines the security level of the system. The highest (most secure) level is level 50. The IBM OS/400 Advanced connector is designed for and has been successfully tested on level 50.

3.4 Configuring the Message Transport Layer

To configure the message transport layer on the IBM OS/400 system, you configure the NOTIFY exit IP address. To do so:

1. Open the QCSRC/IPPARMS file for editing. This file contains the IP address and the port number of the LDAP Gateway. The Notify exit takes the IP address and port number parameters for the LDAP Gateway (installed on the Oracle Identity Manager host computer) from the QCSRC/IPPARMS file.

   The standard port number is 5490. This must be entered as a 6-digit number with zeros preceding the actual port number. For example, 5490 must be entered as `005490`. The port number is followed by the colon (:) symbol, the LDAP Gateway server IP, and then an additional colon symbol. For example:

   ```
   005490:10.0.0.1:
   ```

   The IP address and port number in the QCSRC/IPPARMS file identify the LDAP Gateway to notify real-time changes.

   Note: The port number must take up the first six character positions, with leading zeros in the number. A colon is in the seventh character position. The IP address starts at the eight character position and its size can vary, but it must be followed by a colon.

2. Save the QCSRC/IPPARMS file. This change for IBM OS/400 does not require an IPL.

4

Configuring the Connector

This connector enables real-time reconciliation of user data from the target system. After you deploy the connector and import existing user data from the target system to Oracle Identity Manager, you need not depend on a scheduled task to start reconciliation runs with the target system.

This chapter discusses the following topics:

4.1 Configuring Trusted Source Reconciliation

The XML file for trusted source reconciliation, oimAs400TrustedXellerateUser.xml, contains definitions of the connector components that are used for trusted source reconciliation. To import this XML file:

> **Note:** The procedure described in this section enables trusted source reconciliation for both the initial reconciliation run and subsequent real-time reconciliation runs.

1. Open the Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation pane.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the oimAs400TrustedXellerateUser.xml file, which is in the *OIM_HOME*/XLIntegrations/as400/xml directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the XML file, and then click **OK**.

4.2 Running Initial Reconciliation

The initial reconciliation run involves importing user data from the target system into Oracle Identity Manager, immediately after you deploy the connector.

To start the initial reconciliation run:

1. Ensure that properties that are common to both the run script and the run_initial_recon_provisioning script have the same values.

   The run script is located in the *LDAP_INSTALL_DIR*/bin directory. The run_initial_recon_provisioning script is located in the *OIM_HOME*/JavaTasks directory.

2. In a text editor, open the *OIM_HOME*/JavaTasks/initialAs400Adv.properties file.

3. In the initialAs400Adv.properties file, specify values for the properties that control the initial reconciliation script.

   Note: Ensure that properties that are common to both the initialAs400Adv.properties file and as400Connection.properties file have the same values.

   The properties in the file that control initial reconciliation are:

   - xlAdminId: Oracle Identity Manager administrator ID.
   - idfTrusted: Enter `true` as the value of this property to specify that you want to perform trusted source reconciliation with the target system. Enter `false` to specify target resource reconciliation.
   - _resourceObject_: Resource object for reconciliation.
   - _itResource_: IT resource for target resource reconciliation.
   - isFileRecon: The value for this is `true`, which specifies file-based initial reconciliation. You cannot change this value.
   - userFile: Enter the name of the TXT file in which you have stored the user IDs of the target system users that you want to reconcile. This file must be placed in the *OIM_HOME*/Javatasks directory:

     For more information about this file, see the sample user.txt file in the scripts directory on the installation media.
   - reconAttrs: Fields that are reconciled.
   - idfServerUrl: Enter the LDAP Gateway host and port.

     Note: If you are configuring the LDAP Gateway on the computer on which Oracle Identity Manager is installed, then specify `localhost` as the host name in the value of the idfServerUrl property. If you are configuring the LDAP Gateway on a different computer, then specify the host name or IP address of that computer. However, it is recommended that you install the LDAP Gateway on the same computer on which Oracle Identity Manager is installed.

   You are not allowed to change the values of the rest of the properties in the initialAs400Adv.properties file.

The following is a sample set of values for the properties in the initialAs400Adv.properties file:

```
xlAdminId:xelsysadm
_resourceObject_:OIMAS400AdvResourceObject
_itResource_:AS400AdvResource
idfTrusted:false
isFileRecon:true
userFile:/tmp/user.txt
idfServerUrl:ldap://localhost:5389
idfAdminDn:cn=idfAs400Admin, dc=as400,dc=com
idfAdminPwd:idfAs400Pwd
ouPeople:ou=People
ouGroups:ou=Files
ouBaseDn:dc=as400,dc=com
idfSystemAdminDn:cn=Directory Manager, dc=system,dc=backend
idfSystemAdminPwd:testpass
idfSystemDn:dc=system,dc=backend
reconAttrs:uid,userPassword,text,passwordExpire,status,owner,inlpgm,usrcls,grpp
rf,inlmnu,supgrpprf,jobd,lmtcpb
```

4. In a text editor, open the *OIM_HOME*/JavaTasks/run_initial_recon_provisioning script.
5. To perform trusted source reconciliation:
   a. Set the value of the JV parameter in the script to `-X` to reconcile Xellerate User.
   b. Run the script.

      When you run the script, it opens the file (whose name is the value of the userFile property) containing user data and reads the user IDs of the users that you want to reconcile. Then, the loader, which is the initial load script, connects to the LDAP Gateway and issues commands to fetch the required user data from the target system. This data is loaded in the LDAP Gateway cache and reconciliation events are submitted to Oracle Identity Manager. Xellerate Users are created for all the target system users identified by the userFile property in the initialAs400Adv.properties file.
   c. In the run_initial_recon_provisioning script, change the value of the JV parameter to `-R` to run target resource reconciliation.
   d. Run the script again.

      Because you have set the value of the JV parameter in the script to `-R`, target resource reconciliation is performed when you run the script. Resources are assigned to each OIM User that was created when you first ran the script.
6. To perform target resource reconciliation only:

   Note: Ignore step 6 if you want to run trusted source reconciliation.

   a. In a text editor, open the initialAs400Adv.properties file and enter `false` as the value of the idfTrusted property to specify that you want to perform target resource reconciliation with the target system.

      Make the same change in the as400Connection.properties file.
   b. In the run_initial_recon_provisioning script, change the value of the JV parameter to `-P` to run target resource reconciliation.

c. Run the script again.

Because you have set the value of the JV parameter in the script to `-P`, target resource reconciliation is performed when you run the script.

After the initial reconciliation run ends, real-time reconciliation takes over and newly created or modified user data is automatically reconciled into Oracle Identity Manager.

Note: If you want to configure provisioning and initial reconciliation but not real-time reconciliation, then see step 7 in "Installing and Configuring the LDAP Gateway" on page 2-9.

If a problem exists with fault tolerance and the LDAP Gateway and Reconciliation Agent are down for a long time, and there is a possibility of losing user data, then run full reconciliation.

4.3 Configuring Account Status Reconciliation

When a user is disabled or enabled on the target system, the user is reconciled and the changed status is reflected in Oracle Identity Manager. To configure the reconciliation of account status data:

1. In the *LDAP_INSTALL_DIR* directory, add the name of the status attribute to the reconAttrs section in the as400Connection.properties file.

   Make the same change in the initialAs400Adv.properties file, which is in the *OIM_HOME*/JavaTasks directory.

2. Restart the LDAP Gateway for the changes to take effect.

3. In the Design Console:

   See Also: *Oracle Identity Manager Design Console Guide* for detailed information about the following steps

   - In the OIMAs400ResourceObject resource object, create a field to represent the status attribute.
   - In the OIMAs400ProvisioningProcess process definition, map the field for the status attribute to the OIM_OBJECT_STATUS field.

5

Troubleshooting

This chapter contains the following sections:

5.1 Troubleshooting

Table 5–1 lists solutions to some commonly encountered issues associated with the connector.

Table 5–1 Troubleshooting

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the IBM OS/400 Server.	■ Ensure that the IBM OS/400 server is up and running. ■ Check that the necessary ports are working. ■ View the LDAP Gateway logs to determine if messages are being sent or received. ■ Examine the Oracle Identity Manager configuration to verify that the IP address, admin ID, and admin password are correct. ■ Check with IBM OS/400 platform manager to verify that OS/400 user account and password have not been changed.
OS/400 does not appear to respond.	■ Ensure that the Oracle Identity Manager mappings are correct. ■ Check the configuration mappings for the Advanced Adapter Gateway.
A particular use case does not appear to be functioning.	■ Check for the use case event in question on the LDAP Gateway Server Log. Then check for the event in the specific log assigned to that Advanced Connector. ■ If the event does not register in either of these two logs, investigate the connection between Oracle Identity Manager and the Advanced Connector Gateway. ■ If the event is in the log but the command has not had the intended change on an OS/400 user profile, check for configuration and connections between the LDAP Gateway and IBM OS/400.

5.2 Guidelines on Using the Connector

Apply the following guidelines while using the IBM OS/400 Advanced connector:

- The connector can accept and transmit any non-ASCII data to the mainframe, but the mainframe does not accept non-ASCII characters. As a result, any task that requires non-ASCII data transfer fails. In addition, there is no provision in the

connector to indicate that the task has failed or that an error has occurred on the mainframe. You must exercise caution when providing non-ASCII data to the connector.

- Passwords used on the mainframe must conform to stringent rules related to passwords on mainframes. These passwords are also subject to restrictions imposed by corporate policies and rules about mainframe passwords.
- If you configure the connector for trusted source reconciliation and set the idfTrusted property in the initialAs400Adv.properties file to `true` in one of the target system installations on the mainframe, then it must be set to `true` in all installations that connect to the same LDAP Gateway. Otherwise, the connector will fail. This applies only to a configuration in which a single LDAP Gateway connects to multiple installations of the target system.
- When using any version of IBM OS/400 earlier than 5.4, the Reset Password function for real-time reconciliation is not used. Instead, you can use the User Change Password function.
- The reconciled data may look different than the provisioning data for the following fields:
  - Initial Program (INLPGM)
  - Initial Menu (INLMNU)
  - Job Description (JOBD)

  The reconciliation data displays the expanded value including the entire path, such as /QSYS.LIB/%LIBL%.LIB/MAIN.MNU, and the provisioning data displayed is LIBL/MAIN.

6

Known Issues

The following are the known issues associated with this release of the connector:

- **Bug 7033009**

  The number sign (#) or a space at the *beginning* of the User Profile ID string is not supported. In addition, the following characters are not supported in the User Profile ID string:

  - Comma (,)
  - Plus sign (+)
  - Double quotation mark (")
  - Slash (/)
  - Left angle bracket (<)
  - Right angle bracket (>)
  - Backslash (\)

- **Bug 7353425**

  The connector supports the following default fields for reconciliation and provisioning:

  - UserId
  - Password
  - Password Expire
  - Description Text
  - Initial Program
  - User Class
  - Owner
  - Group Profile
  - Supplemental Group
  - Initial Menu
  - Job Description
  - Limit Capabilities
  - Special Authority

Index

N

O

P

R

S

T

V

X