Oracle® Identity Manager

Connector Guide for IBM i5/OS (OS/400) Advanced

Release 9.0.3

B32447-01

February 2007

Oracle Identity Manager Connector Guide for IBM i5/OS (OS/400) Advanced, Release 9.0.3

B32447-01

Primary Author: Deepa Aswani

Contributing Author: Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for IBM i5/OS (OS/400) Advanced provides information about integrating Oracle Identity Manager with IBM i5/OS (OS/400).

> **Note:** This is a transitional release following Oracle's acquisition of Thor Technologies. Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager IBM i5/OS (OS/400) Advanced Connector.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Connector Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 connector documentation set, 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.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The advanced connector for IBM i5/OS (OS/400) is used to integrate Oracle Identity Manager with IBM i5/OS (OS/400).

> **Note:** Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

The Oracle Identity Manager IBM i5/OS (OS/400) Advanced Connector provides a native interface between IBM i5/OS (OS/400) and Oracle Identity Manager. The advanced connector functions as a trusted virtual administrator on the targeted platform, performing tasks such as creating login IDs, suspending IDs, changing passwords, and performing other functions that administrators usually perform manually.

The IBM i5/OS (OS/400) Advanced Connector enables provisioning and reconciliation to IBM i5/OS (OS/400) security facilities. This chapter discusses the following topics:

- Overview of IBM i5/OS (OS/400) Advanced Connector
- Supported Functionality
- Multilanguage Support
- Files and Directories that Comprise the Connector
- How to Use This Guide

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

Overview of IBM i5/OS (OS/400) Advanced Connector

The IBM i5/OS (OS/400) Advanced Connector includes the following components:

- **i5/OS (OS/400)LDAP Gateway**: The LDAP Gateway receives instructions from Oracle Identity Manager in the same way as any LDAP version 3 identity store. These LDAP commands are then converted into native i5/OS (OS/400) commands and sent to the Provisioning Agent. The response is also native to IBM i5/OS (OS/400), which is then parsed into an LDAP response. After execution, an LDAP-formatted response is returned to the requesting application.
- **i5/OS (OS/400)Provisioning Agent**: The Provisioning Agent is an i5/OS (OS/400) component, receiving native i5/OS (OS/400) provisioning commands from the LDAP Gateway. These requests are processed against the IBM i5/OS (OS/400) authentication repository with the response parsed and returned to the LDAP Gateway.
- i5/OS (OS/400)**Reconciliation Agent**: The Oracle Identity Manager Reconciliation Agent captures native i5/OS (OS/400) events using advanced exit technology for seamless reconciliation to Oracle Identity Manager through the LDAP Gateway. The Reconciliation Agent captures events occurring from the i5/OS (OS/400) logins, command prompt, batch jobs, and other native events in real time. The Reconciliation Agent captures these events and transforms them into notification messages for Oracle Identity Manager through the LDAP Gateway.
- i5/OS (OS/400)**Message Transport Layer**: The message transport layer enables the exchange of messages between the LDAP Gateway and the IBM i5/OS (OS/400) Provisioning and Reconciliation Agent. The i5/OS (OS/400) Advanced Connector uses JTOpen for the message transport layer.

  The Advanced connector is also engineered for high-performance environments and transactions.

> **See Also:** For more information on the IBM i5/OS (OS/400) Advanced Connector architecture and the message transport layer, refer to Appendix B.

Supported Functionality

The following table lists the functions that are available with this connector.

Function	Type	Description
Create i5/OS (OS/400) User	Provisioning	Creates a user
Modify i5/OS (OS/400) User	Provisioning	Modifies a user
Delete i5/OS (OS/400) User	Provisioning	Deletes a user
Change i5/OS (OS/400) Password	Provisioning	Changes the password of a user
Reset i5/OS (OS/400) Password	Provisioning	Resets the user password
Revoke i5/OS (OS/400) User Account	Provisioning	Revokes the user account
Resume i5/OS (OS/400) User Account	Provisioning	Resumes a revoked user account
Assign User to i5/OS (OS/400) Object Permission	Provisioning	Assigns a group permissions to access objects on i5/OS (OS/400) such as the Document Library Object.
List i5/OS (OS/400) Users	Provisioning	Lists all the users

Function	Type	Description
Create User Data Event	Reconciliation	The Reconciliation Agent performs reconciliation when a user is created and data is provided for the user account.
Modify User Data Event	Reconciliation	The Reconciliation Agent performs reconciliation when a user account is modified.
Delete User Event	Reconciliation	The Reconciliation Agent performs reconciliation when a user is deleted.
Password Change Event	Reconciliation	The Reconciliation Agent performs reconciliation when the password of a user is changed.
Disable User Event	Reconciliation	The Reconciliation Agent performs reconciliation when a user account is disabled.
Enable User Event	Reconciliation	The Reconciliation Agent performs reconciliation when a disabled user account is enabled.

The elements that the Reconciliation Agent extracts from the target system to construct reconciliation event records:

- uid
- userPassword
- sn
- cn
- givenName
- status
- owner
- initialProgram
- description
- userControls

See Also: Appendix A, "Attribute Mapping Between Oracle Identity Manager and IBM i5/OS (OS/400)"

Multilanguage Support

This release of the connector supports the following languages:

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean

- Simplified Chinese
- Spanish
- Traditional Chinese

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

Files and Directories that Comprise the Connector

The files and directories that comprise this connector are located in the following directory on the installation media:

```
Security Applications/IBM i5/IBM i5 Advanced Connector
```

Copy the contents of this file to the *oim_home* directory. The contents of this file are described in brief in the following table:

File or Directory on the Installation Media	Description of Files and Contents
`etc/LDAP Gateway/ldapgateway.zip`	Files required for LDAP Gateway deployment on the Oracle Identity Manager system.
`etc/Provisioning and Reconciliation Connector/OIMIDFEX.SAVF`	Connector agent file to be placed on the target system (i5/OS (OS/400) or AS/400) for deployment on the mid-range system.
`lib/as400-adv-provisioning.jar`	Connector JAR file to be deployed on the Oracle Identity Manager system to enable provisioning.
`lib/as400-adv-agent-recon.jar`	Connector JAR file to be deployed on the Oracle Identity Manager system to enable reconciliation.
`lib/as400Connection.properties`	Properties file that specifies controls for the initial reconciliation run between the Oracle Identity Manager system and the target IBM i5/OS (OS/400) system.
Files in the `resources` directory	Each of these files contains locale-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 Administrative and User Console.
`scripts/run_initial_recon_provisioning.sh` `scripts/run_initial_recon_provisioning.bat`	Scripts that perform the initial reconciliation run.
`scripts/run_initial_recon_disable.sh` `scripts/run_initial_recon_disable.bat`	Scripts that perform the initial reconciliation run and further, check for users disabled on the target system and disables them on Oracle Identity Manager
`xml/oimAs400AdvConnector.xml`	The XML file that contains component definitions for the connector.

See Also: The Step 2: Copying the Connector Files section in Chapter 2 for information about copying these files to the appropriate destinations.

How to Use This Guide

The IBM i5/OS (OS/400) Advanced connector deployment primarily consists of installing the LDAP Gateway, Reconciliation Agent, and Provisioning Agent. The LDAP Gateway is installed on the same system as the Oracle Identity Manager server. The Provisioning Agent and Reconciliation Agents are installed on the IBM i5/OS (OS/400) system.

The deployment procedure on the Oracle Identity Manager server is different in nature from the deployment procedure on i5/OS (OS/400). For simplicity, these instructions have been divided into two chapters in this guide:

- Chapter 2, "Deployment on the Oracle Identity Manager Server" covers instructions for deploying the connector on the Oracle Identity Manager system. This consists of configuring the Oracle Identity Manager server, importing the connector XML file, compiling adapters, installing the LDAP Gateway, configuring the message transport layer, and so on.
- Chapter 3, "Connector Deployment on the Target i5/OS (OS/400) System" includes the instructions to deploy the connector on i5/OS (OS/400). While it may be possible for the Oracle Identity Manager administrator to perform these tasks, it is recommended that these tasks be performed with the assistance of the administrator of the IBM i5/OS (OS/400) (earlier IBM AS/400) system.

2

Deployment on the Oracle Identity Manager Server

This chapter covers deploying the connector components on the Oracle Identity Manager server in the following sections:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files
- Step 3: Configuring the Oracle Identity Manager Server
- Step 4: i5/OS (OS/400) Configuring the Connector to Work with the Oracle Identity Manager Application Server
- Step 5: Importing the Connector XML File
- Step 6: Compiling Adapters
- Step 7: Installing and Configuring the LDAP Gateway
- Step 8: Configuring the Message Transport Layer

> **Note:** Chapter 3, "Connector Deployment on the Target i5/OS (OS/400) System" covers the deployment of the connector components on the target i5/OS (OS/400) system.

Step 1: Verifying Deployment Requirements

Verify that the system requirements specified in the following table are met for deploying the IBM i5/OS (OS/400) Advanced Connector.

i5/OS (OS/400)Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target Systems	IBM i5/OS (OS/400) version 4.2 or later
i5/OS (OS/400)i5/OS (OS/400) Repository	IBM i5/OS (OS/400) version 4.2 or later
Target System Host Platform	IBM i5/OS (OS/400) version 4.2 or later
Infrastructure Requirements: message transport layer	JTOpen (Open Source or commercially supported version)
Target system user account for Oracle Identity Manager	i5/OS (OS/400)-authorized account with `System Administrator` privileges

Note: The LDAP Gateway works in a seamless manner with Oracle Identity Manager and operates under the user account created for Oracle Identity Manager on i5/OS (OS/400). As a result, it has the same permissions as those granted to the Oracle Identity Manager user account to access and operate with the Provisioning and Reconciliation Agents.

Step 2: Copying the Connector Files

Copy the following connector files to the destinations on the Oracle Identity Manager server as indicated in the following table.

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:

```
Security Applications\IBM i5\IBM i5 Advanced
```

Refer to the Files and Directories that Comprise the Connector section for more information about these files.

Files	Destination
`etc/LDAP Gateway/ldapgateway.zip`	*`LDAP_install_dir`* The *`LDAP_install_dir`* must be located on the Oracle Identity Manager server.
`lib/as400-adv-agent-recon.jar` `lib/as400Connection.properties`	*`LDAP_install_dir/etc`*

`lib/as400-adv-provisioning.jar`
`scripts/run_initial_recon_provisioning.sh`
`scripts/run_initial_recon_provisioning.bat`
`scripts/run_initial_recon_disable.sh`
`scripts/run_initial_recon_disable.bat`
	oim_home/xellerate/JavaTasks/

Files in the `resources` directory	*oim_home*/xellerate/connectorResources/
`xml/oimAs400AdvConnector.xml`	*oim_home*/xellerate/XLIntegrations/i5OS/xml/

Step 3: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

- Changing to the Required Input Locale
- 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.

Changing to the Required Input Locale

Changing to the required input locale (language and country setting) involves installing the required fonts and setting the required input locale.

To set the required input locale:

> **Note:** Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.
2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the `*oim_home*/xellerate/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, change to the `*oim_home*/xellerate/bin` directory.
2. Enter one of the following commands:

   > **Note:** You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:
   >
   > *oim_home*/xellerate/bin/*batch_file_name*

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   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/xellerate/config/xlConfig.xml

   > **Note:** You can ignore the exception that is thrown when you perform Step 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 informational messages that highlight the progress of the application at 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 still 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:

- **For JBoss Application Server**

  To enable logging:

  1. Uncomment or add the following lines in the `JBoss_home/server/default/conf/log4j.xml` file:

     ```
        <category name="XELLERATE">
           <priority value="<log_level>"/>
        </category>
      log_level= WARN or DEBUG or ALL or INFO or ERROR or FATAL or OFF
     ```

  2. In the properties file, replace *`log_level`* with the log level that you want to set.

     ```
     log4j.logger.XELLERATE=log_level

     log_level= WARN or DEBUG or ALL or INFO or ERROR or FATAL or OFF
     ```

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

  `JBoss_home``/server/default/log/server.log`

- **For IBM WebSphere:**

  To enable logging:

1. Add the following line in the *OIM_home*/xellerate/config/log.properties file:

   ```
   log4j.logger.XELLERATE=log_level
   ```

2. In this line, replace *log_level* with the log level that you want to set.

   For example:

   ```
   log4j.logger.XELLERATE=INFO
   ```

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

```
WebSphere_home/AppServer/logs/server_name/startServer.log
```

- **For BEA WebLogic**

  To enable logging:

  1. Add the following line in the *OIM_home*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     ```

  2. In this line, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=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
  ```

- **For OC4J**

  To enable logging:

  1. Add the following line in the *oim_home*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     ```

  2. In this line, replace *log_level* with the log level that you want to set.

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     ```

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

  ```
  OC4J_home/opmn/logs/default_group~home~default_group~1.log
  ```

Step 4: i5/OS (OS/400) Configuring the Connector to Work with the Oracle Identity Manager Application Server

The IBM i5/OS (OS/400) Advanced connector is compatible with the following application servers:

- JBoss
- IBM WebSphere
- BEA WebLogic
- Oracle Containers for Java (OC4J)

To ensure that the connector works with the application server that Oracle Identity Manager is deployed on, you must the `/ldapgateway/bin/run.sh` file (or `run.bat` for Microsoft Windows) and uncomment the lines related to that particular application server. The following are the contents of the `run.sh` file:

```
SET CLASSPATH VARIABLES
##### SET ENVIRONMENT VARIABLES #######
APP_HOME=/opt/ldapgateway
TMPDIR=/opt/ldapgateway/temp
OIM_HOME=/opt/OIM/xellerate
OIM_CLIENT_LIB=/opt/OIM/client/xlclient/lib

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

##### SET WEBSPHERE HOME ##################
#APPSERVER_HOME=/opt/WebSphere/AppServer/lib

##### SET WEBLOGIC HOME ##################
# APPSERVER_HOME=/opt/bea/

##### SET OC4J HOME ##################
#APPSERVER_HOME=/opt/oracle/oc4j
```

You also need to edit the related application server-specific libraries. For more information, refer to the vendor documentation for the application server.

Step 5: Importing the Connector XML File

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `oimAs400Connector.xml` file, which is in the *`oim_home`*`/xellerate/XLIntegrations/i5OS/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 **Next.** The Provide IT Resource Instance Data page for the `As400Resource` IT resource is displayed.
8. Specify values for the parameters of the `As400Resource` IT resource. Refer to the table in the Defining IT Resources section for information about the values to be specified.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `As400Resource` IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

> **See Also:** If you want to define another IT resource, then refer to *Oracle Identity Manager Tools Reference Guide* for instructions.

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. Remove these nodes by right-clicking each node and then selecting **Remove.**

12. Click **Import**. The connector file is imported into Oracle Identity Manager.

Defining IT Resources

You must specify values for the `As400Resource` IT resource parameters listed in the following table.

Parameter Name	Parameter Value (Default)
Resource Asset Name	`AS400Resource`
Resource Asset Type	`OIMLDAPGatewayResourceType`
Admin Id	`uid=idfAs400Admin,dc=as400,dc=com`
Admin Password	`idfAs400Pwd`
Server Address	`localhost`
Root DN	`dc=as400,dc=com`
Port	`5389`
Is the resource asset to be used to call a method on an API, which resides on a system that is external to Oracle Identity Manager?	`No`

After you specify values for these IT resource parameters, go to Step 9 of the procedure to import connector XML files.

Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- CreateAs400AdvUser
- ChangeAs400AdvUserPassword
- ResetAs400AdvPassword
- DeleteAs400AdvUser
- RevokeAs400AdvUser
- ResumeAs400AdvUser
- ModifyAs400AdvUser
- ModifyRemoveAs400AdvUser

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, select the **Compile All** option.

To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select the **Compile Selected** option.

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*/xellerate/Adapter directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

> **Note:** To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

Step 7: Installing and Configuring the LDAP Gateway

To install and configure the LDAP Gateway on the Oracle Identity Manager server, do the following:

1. Unzip the ldapgateway.zip file to a directory on the Oracle Identity Manager system, referred to as the *LDAP_install_dir*.

   See Also: Step 2: Copying the Connector Files

2. You must configure the LDAP Gateway to use the message transport layer, JTOpen. For this, open the *LDAP_install_dir*/conf/as400.properties file and specify the values for the parameters that are described in following table:

Parameter	Sample Value	Description
host	10.0.0.1	Target i5/OS (OS/400) system IP address
adminId	As400AdminID	Target i5/OS (OS/400) system administrator ID
adminPwd	As400Pwd	Target i5/OS (OS/400) system administrator password
agentHost	10.0.0.1	Target i5/OS (OS/400) system IP address
agentAdminId	As400AgentAdmin	Target i5/OS (OS/400) system reconciliation agent administrator ID
agentAdminPwd	As400AgentAdmPwd	Target i5/OS (OS/400) system reconciliation agent administrator password
agentLib	OIMI5ADV	Target i5/OS (OS/400) system library in which the reconciliation agent files are located
agentFile	QCSRC	Reconciliation agent file on the target i5/OS (OS/400) system
agentMember	EUSRPWD	Reconciliation Agent user with privileges to retrive reconciliation event information

Parameter	Sample Value	Description
`_agentport_`	`5490`	Target i5/OS (OS/400) system port allocated to the reconciliation agent

Step 8: Configuring the Message Transport Layer

The IBM i5/OS (OS/400) Advanced Connector uses JTOpen as the message transport layer to access i5/OS (OS/400) data and resources from the Oracle Identity Manager server. More specifically, it is used by the LDAP Gateway to communicate with the Provisioning and Reconciliation Agents that are installed on the i5/OS (OS/400) system.

> **See Also:** Message Transport Layer in Appendix B, "Connector Architecture"

To configure JTOpen as the message transport layer, do the following:

1. Download JTOpen from the IBM Web site at and unzip the `jtopen_`*`ver`*`.zip` file:

   `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.

3. You also need to configure the LDAP Gateway to use JTOpen as the message transport layer. This is covered in the Step 7: Installing and Configuring the LDAP Gateway section.

3

Connector Deployment on the Target i5/OS (OS/400) System

The Provisioning and Reconciliation Agent Components of the IBM i5/OS (OS/400) Advanced Connector are deployed on IBM i5/OS (OS/400). This chapter describes the installation and configuration of the Provisioning Agent and Reconciliation Agent in the following sections:

- Step 1: i5/OS (OS/400) Verifying Deployment Requirements
- Step 2: i5/OS (OS/400) Installing the Reconciliation Agent
- Step 3: Installing the Exits for the Reconciliation Agent
- Step 4: Configuring the Message Transport Layer

Step 1: i5/OS (OS/400) Verifying Deployment Requirements

The following table identifies hardware, software, and authorization prerequisites for the installing Provisioning Agent and Reconciliation Agent.

Item	Requirement
i5/OS (OS/400) Operating System	IBM i5/OS (OS/400) Verify that all current patches are in place.
Message Transport Layer	JTOpen
i5/OS (OS/400) Identity Repository	Current patch level for i5/OS (OS/400)
Target system user account for the Provisioning Agent and Reconciliation Agent	`SystemAdministrators` privileges on IBM i5/OS (OS/400)

The Provisioning Agent and the Reconciliation Agent are installed on the i5/OS (OS/400). Both require the installation of a started task. In addition, these agents function under a user account on the i5/OS (OS/400) system. This user account must be created by the i5/OS (OS/400) administrator during the deployment of the Provisioning Agent and the Reconciliation Agent.

> **Note:** Both the Provisioning Agent and Reconciliation Agent user accounts require `SystemAdministrators` group privileges on the i5/OS (OS/400).

i5/OS (OS/400) Environmental Settings and Requirements

The Reconciliation Agent operates using user exit technology, outside the i5/OS (OS/400) operating system.

Typical midrange operating system shops install custom exits, for example to maintain a certain password format. The connector exits are engineered to be the last exits called in sequence, allowing existing exits to function normally.

Step 2: i5/OS (OS/400) Installing the Reconciliation Agent

To install the connector on the target IBM i5/OS (OS/400) system, do the following:

1. Do a binary FTP of the `OIMIDFEX.SAVF` file to any directory on the target i5/OS (OS/400) system from the following location:

   ```
   IBM i5 Advanced Connector Rev 9.0.3/etc/Provisioning and
   Reconciliation Connector/OIMIDFEX.SAVF
   ```

2. For this set of instructions, the directory to which this file is transmitted will be referred to as `OIMI5ADV`.

3. To view the saved library and the contained objects, you use the `DSPSAVF` command, as follows:

   ```
   DSPSAVF   FILE(SAMPLIB/OIMIDFEX)

   i5 Screen output from 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

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

4. Now that you know the name and the objects of the saved library, you can restore the objects in the save file using the `RSTOBJ` (restore object) command. Because the restored objects will be saved in a new target library, you need to use the `SAVLIB` and `RSTLIB` parameters. The `SAVLIB` uses the original library name, and `RSTLIB` uses the new library that you restore the save file objects to. The syntax for this command is as follows:

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

If required, the new library can be a general public library (QGPL).

> **Note:** The Provisioning Agent does not require any special configuration during the IBM i5/OS (OS/400) Advanced 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.

Step 3: Installing the Exits for the Reconciliation Agent

After copying the connector save file to the OIMI5ADV library, 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, do the following:

1. The i5/OS (OS/400) Reconciliation Agent can be installed in either a menu-driven or a command-driven installation protocol. The following instructions assume the use of the menu-driven protocol.
2. Log on to the i5/OS (OS/400) system as a system administrator.
3. Ensure that the connector library files and objects are present in the OIMI5ADV library.

   See Also: Step 2: i5/OS (OS/400) Installing the Reconciliation Agent describes the process of copying the connector files to the library.

4. Start the User Exit Registration program WRKREGINF:

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

   In i5/OS (OS/400), exit programs are called dynamically. This means that if an exit program was registered with the system, you can replace the program with a new version, without the need to register the exit.

5. You will primarily work with the CHG_PROFILE (change), CRT_PROFILE (create), and DLT_PROFILE (delete) entries. Deleting a user profile can be a lengthy affair, because a user may own multiple objects, and therefore, be present on many lists and internal tables.

   Cleaning up after a user can take a long time to process (many minutes), so a batch job is used for the clean-up process. There are two delete points: before the start of the clean-up job, and at the end of the clean-up job. The Reconciliation Agent monitors only the first delete point (before the clean-up job).

   In addition, 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. In the following example, option 8 is selected for these exit points, either as a group or one at a time. The following exits will be changed:

   ```
   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
   ```

6. You also need the RST_PROFILE (restore) exit point, which is used when user profiles are restored from a save file during otherwise normal operation (and not during a restore of the whole system from scratch).

   You also need to use the VLD_PASSWRD exit point, which is called when the password is changed by the user. This 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.

   > **Note:** This IBM design limitation has been fixed in IBM i5/OS (OS/400) V5R4 by introducing another exit point called QIBM_QSY_CHK_PASSWRD.

7. You need to register the XUSRPWD exit program with QIBM_QSY_CHG_PROFILE. However, when you try to do this, you might find that there is an existing exit program registered for this point. In the following code snippet, this is QGLDPUEXIT in the main system library QSYS. This implies that the i5/OS (OS/400) system itself uses this exit point to extend its functionality.

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

```
               Exit
             Program     Exit
Opt           Number     Program        Library
1                        XUSRPWD        OIMI5ADV
         2147483647      QGLDPUEXIT     QSYS
```

8. Press the Enter key, and the Add screen appears. The screen should have 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  . . . . . . . . . >   OIMI5ADV  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, then the F5 key to refresh the system to view the result of the procedure.

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

9. Proceed with the remaining exit points as follows:

```
             Program     Exit
 Opt          Number     Program        Library

                   1     XUSRPWD        OIMI5ADV
          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 i5/OS (OS/400) V5R4, you also register the CHK_PASSWRD exit point.

10. Before the General Registration Facility was introduced, a password validation program was used. This was handled through the system value settings. The command WRKSYSVAL allows you to work with the system values that control most of the system configuration. Enter the command WRKSYSVAL and scroll down to the following line:

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

11. Select option 2 for QPWDVLDPGM.
12. After the XUSRPWD exit program is added to the various exit points, the NOTIFY exit program must be added as well. The NOTIFY exit program needs to be defined with Program Number 2, because it must be triggered after the XUSRPWD exit program. The NOTIFY exit program needs to be registered only for the CHGP0100, CRTP0100, and DLTP0200 exits.
13. This completes the installation of the reconciliation agent exits.

Note:

- If an exit program is specified instead of *REGFAC, do not continue, as you will interfere with an existing validation program. This way of specifying a validation program is now obsolete. The calling format is different from that of the registered programs and is no longer found in recent documentation. The IBM i5/OS (OS/400) Advanced connector code does not support the old-style validation program.
- The QSECURITY system value determines the security level of the system. The highest (most secure) level is level 50. The Oracle Identity Manager i5/OS (OS/400) Advanced Connector has been designed for and has been successfully tested on level 50, the highest security level.

Step 4: Configuring the Message Transport Layer

To configure the message transport layer on the i5/OS (OS/400) system, you configure the Notify exit IP address.

1. The Notify exit takes the IP address and port number parameters for the LDAP Gateway (installed on the Oracle Identity Manager server) from the `QCSRC/IPPARMS` file.
2. To specify the IP address and the port number of the LDAP Gateway, open the `QCSRC/IPPARMS` file for editing.
3. 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`.
4. 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:
   ```

5. Save the `QCSRC/IPPARMS` file. This change for the IBM i5/OS (OS/400) does not require an IPL.

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.

4

Initial Reconciliation Run

Reconciliation with the IBM i5/OS (OS/400) Advanced connector is carried out in real time. This implies that after you have imported the initial load of user information, you need not perform reconciliation as a scheduled task. The initial reconciliation run involves obtaining user information from the target system, to allow extension of enterprise user management of profiles and authorization of resources.

The initialization process is run from the command line on the Oracle Identity Manager server. The commands are run from the *oim_home*/xellerate/JavaTasks directory. There are non-trusted example scripts for initial provisioning and initial disabling at the following location:

```
IBM i5 Advanced Rev 9.0.3/scripts
```

These non-trusted scripts are:

```
run_initial_recon_provisioning.bat
run_initial_recon_disable.bat
```

The controls for the commands in these files are specified in the initialAs400Adv.properties file. The following is a sample set of values for these parameters:

```
xlAdminId:xelsysadm
xlAdminPwd:xelsysadm
xlJndiUrl:jnp://localhost:1099
xlJndiFactory:org.jnp.interfaces.NamingContextFactory
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
XellerateUserResourceObject:Xellerate User
As400AdvancedResourceObjecct:OIMAS400AdvResourceObject
xlJndiUrlWebSphere:corbaloc:iiop:localhost:2809
xlJndiFactoryWebsphere:com.ibm.websphere.naming.WsnInitialContextFactory
```

To include or exclude specific users during initial reconciliation, modify the following lines:

```
idfIgnoreIdList:start1,start2,private
idfDoOnlyIdList:jdoe81,jdoe82,jdoe83
```

> **Note:** This control does not support wildcards and is designed for processing or excluding a limited number of users.

Configuring Trusted Source Reconciliation

To configure the connector to perform trusted source reconciliation, set the `idfTrusted` control in the `connection.properties` file to `true`, as follows:

```
idfTrusted:true
```

This control toggles trusted source reconciliation in the connector. Set this to `false` if you are not performing reconciliation with a trusted source.

Also, make a copy of the non-trusted scripts and change the `JV` parameter first to `–X` then to `–R`. These scripts can now be used for trusted source reconciliation.

> **Note:** Reconciliation updates to Oracle Identity Manager are in real-time. Therefore, you do not need to configure reconciliation as a scheduled task on Oracle Identity Manager after you have performed the initial reconciliation run.
>
> Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

5

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter contains information on the following types of testing:

- **Provisioning Testing:** This type of test involves using Oracle Identity Manager for provisioning or de-provisioning one of its users or organizations with a target resource. In other words, Oracle Identity Manager is the starting point of the connector, and the target resource is the end point.
- **Reconciliation Testing:** In this type of test, you reconcile Oracle Identity Manager with the target resource. In other words, the target resource is the starting point of the connector, and Oracle Identity Manager is the end point.

This chapter contains the following sections:

- Running Test Cases
- Troubleshooting
- Performance Tests

Running Test Cases

This section focuses on the functional and performance test cases that are associated with this connector. The following table includes information on running test cases on the IBM i5/OS (OS/400) Advanced connector:

Test Case	Test Type	Description/Comment
Test to change IBM i5/OS (OS/400) Password	Provisioning	A user password is changed, with the change posted to i5/OS (OS/400) through the connector.
Test to reset IBM i5/OS (OS/400) Password	Provisioning	A user password is reset, with the change posted to i5/OS (OS/400) through the connector.
Test to create IBM i5/OS (OS/400) user	Provisioning	A user is created, with the change posted to i5/OS (OS/400) through the connector.
Test to revoke or disable IBM i5/OS (OS/400) user account	Provisioning	A user account is revoked, with the change posted to i5/OS (OS/400) through the connector.
Test to resume IBM i5/OS (OS/400) user account	Provisioning	A user account is resumed from a revoked status, with the change posted to i5/OS (OS/400) through the connector.
Test to list IBM i5/OS (OS/400) users	Provisioning	A list of users is retrieved from i5/OS (OS/400) i5/OS (OS/400) repository.

Test Case	Test Type	Description/Comment
Test to permit IBM i5/OS (OS/400) user access to resource profile	Provisioning	A user is authorized to access i5/OS (OS/400) resources, with change posted to i5/OS (OS/400) through the connector.
Test to permit IBM i5/OS (OS/400) user access to TSO	Provisioning	A user is provisioned to log on to i5/OS (OS/400) through TSO, with the change posted to i5/OS (OS/400) through the connector.
Test to remove IBM i5/OS (OS/400) user access to dataset	Provisioning	A user is removed from access to an i5/OS (OS/400) dataset, with the change posted to i5/OS (OS/400) through the connector.
Test to remove IBM i5/OS (OS/400) user access to resource profile	Provisioning	A user is removed from access to an i5/OS (OS/400) resource, with the change posted to i5/OS (OS/400) through the connector.
Test to detect and report native IBM i5/OS (OS/400) password change event	Reconciliation	A native password change is made on i5/OS (OS/400) and subsequently detected by the connector.
Test to detect and report native IBM i5/OS (OS/400) password reset event	Reconciliation	A native password reset is made on i5/OS (OS/400) and subsequently detected by the connector.
Test to detect and report Native IBM i5/OS (OS/400) create user data event	Reconciliation	user creation is done by an administrator natively on i5/OS (OS/400) and subsequently detected by the connector.
Test to detect and report native IBM i5/OS (OS/400) revoke user event	Reconciliation	A user account password is revoked through native i5/OS (OS/400) events, which is subsequently detected by the connector.
Test to detect and report native IBM i5/OS (OS/400) delete user event	Reconciliation	A user account is deleted through native i5/OS (OS/400) events, which is subsequently detected by the connector.
Test to detect and report native IBM i5/OS (OS/400) resume user event	Reconciliation	A user account is resumed from a revoke status through native i5/OS (OS/400) events, which is subsequently detected by the connector.

Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the IBM i5/OS (OS/400) Advanced Connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the IBM i5/OS (OS/400) Server.	■ Ensure that the i5/OS (OS/400) server is up and running. ■ Check that the necessary ports are working. ■ View the 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 i5/OS (OS/400) platform manager to verify that i5/OS (OS/400) user account and password have not been changed.

Problem Description	Solution
i5/OS (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 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 i5/OS (OS/400) user profile, check for configuration and connections between the Gateway and i5/OS (OS/400).

Performance Tests

The IBM i5/OS (OS/400) Advanced Connector architecture has been engineered for enterprise-level performance. When an identity event passes through an exit, the Reconciliation Agent analyzes the event, and then creates a message, allowing the command to complete its routine without loss of time.

The LDAP Gateway is engineered to detect when a given event originates from Oracle Identity Manager, when it passes through the Reconciliation Connector. Provisioning Agent events also create a native exit event that is detected. To prevent a feedback loop, events that originate from the LDAP Gateway are logged, but are not reported again to Oracle Identity Manager. By contrast, events that originate outside Oracle Identity Manager are treated as native events, and recorded for future auditing.

The LDAP Gateway and Reconciliation securely capture, filter, and log the identity events from the host system, publishing them for use by Oracle Identity Manager.

6 Known Issues

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

- The IBM i5/OS (OS/400) Advanced Connector can accept and transmit any non-ASCII data to the i5/OS (OS/400), but the i5/OS (OS/400) may 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 i5/OS (OS/400). You must exercise caution when providing inputs to the connector for the target system, especially when using a regional language interface.
- Passwords used on the i5/OS (OS/400) must conform to stringent rules related to passwords on i5/OS (OS/400). These passwords are also subject to restrictions imposed by corporate policies and rules about i5/OS (OS/400) passwords. While creating user accounts for target systems on the i5/OS (OS/400), you must take these requirements into account before assigning passwords for these accounts.
- This only applies to a configuration where a single LDAP Gateway connects to multiple installations of the target system. If you configure the connector for trusted source reconciliation and set the `idfTrusted` parameter to true in one of the target system installations on the i5/OS (OS/400), then it must be set to true in all installations that connect to the same Gateway. Otherwise, the connector will fail to work.
- When using any version of i5/OS (OS/400) earlier than 5.4, the Reset Password function for real-time reconciliation is not used, and the User Change Password function is used instead.

A

Attribute Mapping Between Oracle Identity Manager and IBM i5/OS (OS/400)

The following tables describe the schema used by the Oracle Identity Manager LDAP Gateway.

- Table A–1, " User Attribute Descriptions"
- Table A–2, " Dataset Resource Profile Attribute Descriptions"

Table A–1 User Attribute Descriptions

Oracle Identity Manager Gateway Attribute	IBM i5/OS (OS/400) Attribute	Description
uid	USER	User login ID
cn	NAME	User full name
sn	NAME	User last name
givenName	NAME	User first 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
userControls	USRCLS	Special access control for the user
initialProgram	INLPRG	User initial program
description	TEXT	Free form text field

Table A–2 Dataset Resource Profile Attribute Descriptions

Oracle Identity Manager Attribute	IBM i5/OS (OS/400) Attribute	Description
cn	PROFILE NAME	The profile id
standardAccessList	ID,ACCESS,ACCESS COUNT	The standard access list of IDs and access for the dataset
conditionalAccessList	ID,ACCESS,ACCESS COUNT	The conditional access list of IDs and access for the dataset
owner	OWNER	The owner of the dataset
auditing	AUDITING	Indicates whether auditing should be enabled

Table A–2 (Cont.) Dataset Resource Profile Attribute Descriptions

Oracle Identity Manager Attribute	IBM i5/OS (OS/400) Attribute	Description
notify	NOTIFY	Indicates whether notification is enabled for any changes to resource profiles
instdata	DATA	The installation data for the dataset

B

Connector Architecture

This appendix describes the i5/OS (OS/400) IBM i5/OS (OS/400) Advanced Connector functionality in detail in the following sections:

- Oracle Identity Manager LDAP Gateway
- Oracle Identity Manager Provisioning Agent
- Oracle Identity Manager Reconciliation Agent
- Message Transport Layer

Oracle Identity Manager LDAP Gateway

The architecture for Oracle Identity Manager Advanced Connector begins with the Oracle Identity Manager LDAP Gateway. The LDAP Gateway is built on Java 1.4.2, allowing for portability across different platforms and operating systems and complete integration with the Oracle Identity Manager system.

The LDAP Gateway works transparently with Oracle Identity Manager to communicate with IBM i5/OS (OS/400) facilities. The LDAP Gateway is installed along with Oracle Identity Manager on the same server. In addition, the Reconciliation Agent enables the LDAP Gateway server to become a subscriber to security and identity events from IBM i5/OS (OS/400).

Oracle Identity Manager maps midrange authentication repositories by the LDAP DN. By changing the LDAP DN, different authentication repositories and different target system resources can be addressed.

Oracle Identity Manager Provisioning Agent

The Provisioning Agent is an i5/OS (OS/400) component, receiving native IBM i5/OS (OS/400) Advanced provisioning commands from the LDAP Gateway. These requests are processed against the IBM i5/OS (OS/400) Advanced authentication repository with the response parsed and returned to the LDAP Gateway.

The Provisioning Agent includes LDAP bind and authorization requests. In addition to traditional provisioning functions, the Provisioning Agent can also build the necessary i5/OS (OS/400) logon functions and working to replicate existing i5/OS (OS/400) user profile scenarios.

The Provisioning Agent receives Identity and Authorization change events, and effects requested changes on the i5/OS (OS/400) midrange authentication repository.

Oracle Identity Manager Reconciliation Agent

When an event occurs on i5/OS (OS/400), independent of any custom installed technology, the event is processed through an appropriate i5/OS (OS/400) exit. Because the Reconciliation Agent uses exit technology, there are no hooks in the i5/OS (OS/400) operating system.

Identity events that arise from a user at i5/OS (OS/400) login, changes by an administrator from the command prompt, or events resulting from batch jobs are detected and notification messages are securely sent in real time. The Reconciliation Agent captures changes to user attributes, changes to a user account, and certain changes to user authorization for libraries and resources. If a user account is created or deleted on i5/OS (OS/400), the Reconciliation Agent will notify Oracle Identity Manager and even create a corresponding account in Oracle Identity Manager.

Passwords fall into a special category. If business rules permit, a password change will be passed to Oracle Identity Manager in clear text and real time. In a testing environment, it is almost immediate. Within other business rules, only a notification that the password has been changed will be passed.

The Reconciliation Agent sends notification events to the LDAP Gateway from i5/OS (OS/400). This architecture does not originate with IBM i5/OS (OS/400), but captures the events just outside the operating system using exit technology, in real time.

A command execution is passed through an exit, just before full completion of the native i5/OS (OS/400) command. A common use of this technology is to require user accounts or passwords to be formatted to a proper length or that they must contain at least one letter and one number. If the exit fails, the command fails and returns an error message. By capturing identity or authentication events at an exit, the Reconciliation Agent captures these events just prior to completing the command and storing the results in the IBM i5/OS (OS/400) Advanced authentication repository.

Message Transport Layer

JTOpen is a library of Java classes that allow you to implement the client-server and internet programming model with an i5/OS (OS/400) system. The JTOpen classes can be used by Java applets, servlets, and applications to access data and resources on an i5/OS (OS/400) system. JTOpen requires only the Java Virtual Machine (JVM) and the Java Developer Kit (JDK).

Functionally, JTOpen is the same as IBM Toolbox for Java. In addition to being Open Source, JTOpen is IBM's effort to get fixes and enhancements out to customers as soon as possible without being constrained by release schedules and other such factors.

Note: For more information on the JTOpen project and IBM's role in the effort, refer to the JTOpen project home page at:

http://jt400.sourceforge.net/

See Also: For more information on JTOpen functionality, refer to the IBM Toolbox for Java documentation at the following location:

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

Index