Oracle® Identity Manager

Connector Guide for IBM AS/400 Advanced

Release 9.0.4

E10452-11

July 2014

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

E10452-11

Primary Author: Gowri.G.R

Contributing Author: Prakash Hulikere, Gauhar Khan, Deena Purushothaman

Contents

2 Connector Deployment on Oracle Identity Manager

3 Connector Deployment on the iSeries

4 Using the Connector

5 Extending the Functionality of the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with IBM AS/400.

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

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

For generic information about connectors, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manage*r.

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

`http://docs.oracle.com/cd/E11223_01/index.htm`

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, visit Oracle Technology Network at `http://www.oracle.com/technetwork/indexes/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 AS/400?

This chapter provides an overview of the updates made to the software and documentation for the Oracle Identity Manager Connector for IBM AS/400 in release 9.0.4.16.

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 sections discuss software updates:

- Updates in Releases 9.0.4.1 Through 9.0.4.4
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.13
- Software Updates in Release 9.0.4.14
- Software Updates in Release 9.0.4.15
- Software Updates in Release 9.0.4.16

Updates in Releases 9.0.4.1 Through 9.0.4.4

The following are software updates in releases 9.0.4.1 through 9.0.4.4:

- IBM AS/400 user profile commands supported by the Provisioning Agent have been added in "Supported Functions for Provisioning" on page 1-8.
- The list of functions supported by the Provisioning Agent has been updated in "Supported Functions for Provisioning" on page 1-8.
- The commands supported by the Reconciliation Agent have been updated in "Supported Functions for Target Resource and Trusted Source Reconciliation" on page 1-8.

- The list of functions supported by the Reconciliation Agent has been updated in "Supported Functions for Target Resource and Trusted Source Reconciliation" on page 1-8.
- The list of fields reconciled between Oracle Identity Manager and IBM AS/400 has been updated in "User Attributes for Target Resource Reconciliation and Provisioning" on page 1-9.
- 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 5-6.
- 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 7, "Known Issues":
  - Bug 7189194
  - Bug 7353425

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for Configuring a Single LDAP Gateway to Work with Multiple Installations of the Target System
- Support for Reconciliation Through a Scheduled Task

Support for Configuring a Single LDAP Gateway to Work with Multiple Installations of the Target System

In the earlier release, one installation of the LDAP Gateway worked with one target system installation. If you had multiple target system installations, you had to install multiple LDAP Gateways. From this release onward, you can configure a single LDAP Gateway to work with multiple target system installations. See Section 5.5.1, "Configuring One LDAP Gateway for Each Installation of the Target System" for more information.

This item was tracked by Bug 9483766.

Support for Reconciliation Through a Scheduled Task

The User Target Recon Scheduled Task scheduled task has been introduced in this release. You can configure this scheduled task to schedule reconciliation with the target system. See Section 4.1, "Configuring Reconciliation" for information about using this scheduled task. In addition, the Last Modified Time Stamp parameter has been added in the IT resource definition. See Section 2.5, "Configuring the IT Resource" for information about this parameter.

This item was tracked by Bug 9483766.

Software Updates in Release 9.0.4.13

The following are the software updates in release 9.0.4.13:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

- Resolved Issues in Release 9.0.4.13

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 4.4.2, "Request-Based Provisioning" for more information.

Resolved Issues in Release 9.0.4.13

The following table lists issues resolved in release 9.0.4.13:

Bug Number	Issue	Resolution
9231097	At the end of a successful Delete User provisioning operation, the connector showed the status R (that is, Rejected) instead of C (Completed).	This issue has been resolved. The connector now shows status C at the end of a successful Delete User provisioning operation.
10070632 and 9866401	Initial reconciliation did not work correctly.	This issue has been resolved. Initial reconciliation now works as expected.
9937520	The connector could not be used to manage more than one supplemental group.	This issue has been resolved. The connector can now be used to manage multiple supplemental groups.
9934948	The password of the target system user account used for connector operations could be viewed in plaintext in the LDAP Gateway.	This issue has been resolved. The password is not stored in the LDAP Gateway.
7356959	Under certain conditions, a Delete User provisioning operation resulted in the creation of a Delete User reconciliation event.	This issue has been resolved. A Delete User provisioning operation does not cause the creation of a Delete User reconciliation event.
7353425	The connector did not support some standard IBM AS/400 attributes.	This issue has been resolved. All standard IBM AS/400 attributes are now supported. In addition, you can add new attributes for reconciliation and provisioning. Section 5.1, "Adding New Attributes for Target Resource Reconciliation" describes the procedure.
7272110	During trusted source reconciliation, when an OIM User is created for a user that is in the Disabled state on the target system, the OIM User is not in the Disabled state.	This issue has been resolved. When an OIM User is created for a user that is in the Disabled state on the target system, the OIM User is also in the Disabled state.

Software Updates in Release 9.0.4.14

The following is the software update in release 9.0.4.14:

From this release onward, reconciliation using external .jar files is no longer supported. Instead, both initial and real-time reconciliation are performed by running the scheduled task.

See Section 4.1, "Configuring Reconciliation" for detailed instructions.

Software Updates in Release 9.0.4.15

The following are the software updates in release 9.0.4.15:

- Support for ignoreEvent() During Reconciliation
- Support for SSL Configuration in LDAP Gateway
- Support for new IT Resource Parameters and LDAP Gateway Properties

Support for ignoreEvent() During Reconciliation

From this release onwards, the connector supports the Oracle Identity Manager reconciliation API feature ignoreEvent(). The LDAP Gateway will now confirm whether a reconciliation event should be ignored prior to creating the event in Oracle Identity Manager. Both real-time reconciliation and full reconciliation utilize this feature. See Section 1.4.2.1, "Full Reconciliation Process," and Section 1.4.2.3, "Incremental (Real-Time) Reconciliation Process," for more details.

Support for SSL Configuration in LDAP Gateway

From this release onwards, SSL configuration in LDAP Gateway has been supported. See Section 2.9, "Installing and Configuring the LDAP Gateway," for more information.

Support for new IT Resource Parameters and LDAP Gateway Properties

From this release onwards, the connector supports new IT resource parameters and LDAP gateway properties. See Table 2–2 and Table 2–3 for more details.

Resolved Issues in Release 9.0.4.15

The following table lists issues resolved in release 9.0.4.15

Bug Number	Issue	Resolution
14164429	The Oracle Identity Manager 11G cannot connect to LDAPGATEWAY provided by OS400 connector.	This issue has been resolved. The Oracle Identity Manager 11G can now successfully connect to the LDAPGATEWAY.
12987614	AS 400 connector feature cannot run a CPYUSRPR command on the target system.	This issue has been resolved. The CPYUSRPR command on the target system can be run and can configure the LDAP and OIM adapters.

Software Updates in Release 9.0.4.16

The following are the software updates in release 9.0.4.16:

- Additional Features for Scheduled Task- User Reconciliation
- Support for Scheduled Task- Single Connection User Reconciliation
- Support for Scheduled Task- Delete User Reconciliation Using LDAP
- Support for Scheduled Task- Delete User Reconciliation Using Oracle Identity Manager

Additional Features for Scheduled Task- User Reconciliation

From this release onward, the user reconciliation scheduled task supports the "LDAP Time Zone" property. This property can be used to specify the local time zone of the LDAP server machine in cases where Oracle Identity Manager and the LDAP gateway are hosted on separate servers in separate time zones. See Section 4.1, "Configuring Reconciliation," and Section 5.4, "Using the Additional Reconciliation Scheduled Tasks" for more details.

Support for Scheduled Task- Single Connection User Reconciliation

From this release onward, the connector supports an additional scheduled task for user profile reconciliation. This task creates a single connection to the target system and retrieves both user IDs and the user's profile attributes. Each user is stored in the internal LDAP store, if needed, and then those users are reconciled to Oracle Identity Manager. See Section 5.4, "Using the Additional Reconciliation Scheduled Tasks" for more details.

Support for Scheduled Task- Delete User Reconciliation Using LDAP

From this release onward, the connector supports an additional scheduled task for reconciling deleted users on the target system. This task retrieves a list of users from the target system and compares that list with a list of users from the internal LDAP store. If a user is found to exist within the internal LDAP store, but not on the target system, then the internal LDAP store is updated and a delete reconciliation event for the user is sent to Oracle Identity Manager. See Section 5.4, "Using the Additional Reconciliation Scheduled Tasks" for more details.

Support for Scheduled Task- Delete User Reconciliation Using Oracle Identity Manager

From this release onward, the connector supports an additional scheduled task for reconciling deleted users on the target system. This task retrieves a list of users from the target system and compares that list with a list of users from Oracle Identity Manager. If a user is found to exist within Oracle Identity Manager, but not on the target system, then a delete reconciliation event for the user is sent to Oracle Identity Manager. See Section 5.4, "Using the Additional Reconciliation Scheduled Tasks" for more details.

Resolved Issues in Release 9.0.4.16

The following table lists issues resolved in release 9.0.4.16

Bug Number	Issue	Resolution
15988796	Reconciliation failing due to special characters (such as #) in UID.	This issue has been resolved. The LDAP gateway now supports UIDs that begin with special characters.
15988779	Connector updates the date on IT Resource are not time zone transparent.	This issue has been resolved. All scheduled tasks now include an "LDAP Time Zone" property that specifies the local time zone of the LDAP gateway server.
14679339	User profile attribute USEDATE is not made available for reconciliation on the gateway.	This issue has been resolved. The USEDATE property is now supported.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4
- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.13
- Documentation-Specific Updates in Release 9.0.4.14
- Documentation-Specific Updates in Release 9.0.4.15

- Documentation-Specific Updates in Release 9.0.4.16

Documentation-Specific Updates in Releases 9.0.4.1 Through 9.0.4.4

The following are software updates in releases 9.0.4.1 through 9.0.4.4:

- The "Certified Components" section on page 1-2 has been updated with specific IBM AS/400 versions that can be used to deploy the Oracle Identity Manager IBM AS/400 Advanced connector.
- The user profile field mappings between Oracle Identity Manager and the target system have been added in "User Attributes for Target Resource Reconciliation and Provisioning" on page 1-9. "Appendix A: Attribute Mapping Between Oracle Identity Manager and IBM i5/AS" has been removed.
- The components of the IBM AS/400 Advanced connector and the connector architecture for reconciliation and provisioning have been added in "Connector Architecture" on page 1-3. "Appendix B: Connector Architecture" has been removed.
- Guidelines that were earlier documented in Chapter 7, "Known Issues" have been moved to "Guidelines on Using the Connector" on page 4-4.
- In "Certified Languages" on page 1-2, Arabic has been added to the list of languages that the connector supports.
- In "Certified Components" on page 1-2, changes have been made in the "Target System" row. Information about certified deployment configurations has been removed from "Certified Components" on page 1-2.
- In "Certified Components" on page 1-2, the minimum Oracle Identity Manager release has been changed to 9.1.0.1 and the JDK requirement of release 1.5 or later has been added.

Documentation-Specific Updates in Release 9.0.4.12

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.13

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.14

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.15

The following are the documentation-specific updates in release 9.0.4.15:

- Table 2–1 has been updated for file or directory on the installation media.
- A new Section 2.3, "Before Running the Connector Installer" has been added.
- Table 4–1 has been updated for new attributes.

Documentation-Specific Updates in Release 9.0.4.16

The following are the documentation-specific updates in revision "10" of release 9.0.4.16:

- Table 4–1 has been updated for new attributes.
- Table 2–3 has been updated for new properties.

- A new Section 5.4, "Using the Additional Reconciliation Scheduled Tasks" has been added on reconciliation scheduled tasks.

The following are the documentation-specific updates in revision "11" of release 9.0.4.16:

- The "Oracle Identity Manager" row of Section 1.1, "Certified Components" has been modified.
- Section 1.2, "Usage Recommendation" has been added.

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 external, identity-aware applications. This guide discusses the connector that enables you to use IBM AS/400 either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

The advanced connector for IBM AS/400 provides a native interface between IBM AS/400 and Oracle Identity Manager. The connector functions as a trusted virtual administrator on the target system, performing tasks related to creating and managing user profiles.

In the account management (target resource) mode of the connector, information about users created or modified directly on the target system is reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

In the IBM AS/400 context, the term "user profile" is synonymous with "user account." If IBM AS/400 is configured as a target resource, then user profiles on IBM AS/400 correspond to accounts or resources assigned to OIM Users. In contrast, if IBM AS/400 is configured as a trusted source, then user profiles on IBM AS/400 correspond to OIM Users.

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

This chapter is divided into the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Usage Recommendation"
- Section 1.3, "Certified Languages"
- Section 1.4, "Connector Architecture"
- Section 1.5, "Features of the Connector"

- Section 1.6, "Connector Objects Used During Reconciliation and Provisioning"

1.1 Certified Components

Table 1–1 lists the certified components.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	■ Oracle Identity Manager Release 9.1.0.1 and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector supports. ■ Oracle Identity Manager 11*g* Release 1 (11.1.1.3.0) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 11.1.1.3.0 and future releases in the 11.1.1.*x* series that the connector supports. ■ Oracle Identity Manager 11*g* Release 1 PS1 (11.1.1.5.0) and any later BP in this release track
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or later. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later.
Target System	IBM i5/AS and AS/400 releases V5R2, V5R3, V5R4, V6R1
Infrastructure Requirements: Message transport layer between the Oracle Identity Manager and the mainframe environment	JTOpen versions 5.1.1 and 5.2 (open source or commercially supported version)
Target system user account for Oracle Identity Manager	IBM AS/400-authorized account with SystemAdministrators privileges Section 2.9, "Installing and Configuring the LDAP Gateway" describes the procedure to specify the credentials of this user.

1.2 Usage Recommendation

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:

- If you are using an Oracle Identity Manager release that is 9.1.0.1 or later and earlier than Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0), then use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) or later, then use the latest 11.1.1.*x* version of this connector.

1.3 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)

- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

> **See Also:** On Oracle Identity Manager release 9.1.0.*x*, see *Oracle Identity Manager Globalization Guide*.
>
> On Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

1.4 Connector Architecture

The connector architecture is described in the following sections:

- Section 1.4.1, "Connector Components"
- Section 1.4.2, "Connector Operations"

1.4.1 Connector Components

The connector contains the following components:

- **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 commands for IBM AS/400 and sent to the Provisioning Agent. The response, which is also native to IBM AS/400, is parsed into an LDAP-format response and returned to Oracle Identity Manager.
- **JTOpen Provisioning Agent:** The connector provides the provisioning functionality through the JTOpen Provisioning Agent. The Provisioning Agent receives IBM AS/400 identity and authorization change events from the LDAP Gateway. These events are processed against the IBM AS/400 authentication repository, in which all provisioning updates from the LDAP Gateway are stored. The response is parsed and returned to the LDAP Gateway.
- **Message Transport Layer:** The message transport layer enables the exchange of messages between the LDAP Gateway and the Provisioning Agent. JTOpen is used as the messaging protocol for the message transport layer.

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

1.4.2 Connector Operations

This section provides an overview of the following connector processes:

- Section 1.4.2.1, "Full Reconciliation Process"
- Section 1.4.2.2, "Incremental Reconciliation Process"
- Section 1.4.2.3, "Incremental (Real-Time) Reconciliation Process"
- Section 1.4.2.4, "Provisioning Process"

1.4.2.1 Full Reconciliation Process

Full reconciliation involves fetching existing user profile data from the mainframe to Oracle Identity Manager. If you configure the target system as a target resource, then the user profile data is converted into accounts or resources for OIM Users. If you configure the target system as a trusted source, then the user profile data is used to create OIM Users.

The following is a summary of the full reconciliation process:

Note: Detailed instructions are provided later in this guide.

1. You specify the full reconciliation configuration in the AS400 User Reconciliation scheduled task (located in the Oracle Identity Manager 9.x Design console).
2. In the scheduled task form, you enter a list of user IDs of the user profiles that you want to reconcile. If no users are specified, then all existing users on the target system will be reconciled.
3. You specify whether you want to configure IBM AS/400 as a target resource or trusted source of Oracle Identity Manager.
4. You set a start time for the task and run the scheduled task. The task sends the list of user IDs to the LDAP Gateway.
5. The LDAP Gateway encrypts the list of user IDs and then sends it to the Provisioning Agent on the mainframe. The user ID and status of each user profile is stored in an internal meta-store, and a flag is set for the user profile in the meta-store.
6. The Provisioning Agent encrypts user profile data for the specified user IDs and then passes this data to the LDAP Gateway.
7. The LDAP Gateway decrypts the user profile data and passes it to Oracle Identity Manager.
8. The next step depends on the setting in the scheduled task:

- If you configure the target system as a target resource, then the user profile data is converted into accounts or resources assigned for OIM Users.
- If you configure the target system as a trusted source, then the user profile data is used to create OIM Users.

1.4.2.2 Incremental Reconciliation Process

The following is a summary of the incremental reconciliation process:

1. IBM AS/400 identity and authorization events take place in the target system. After each event, the modified time stamp on the changed profile is updated.

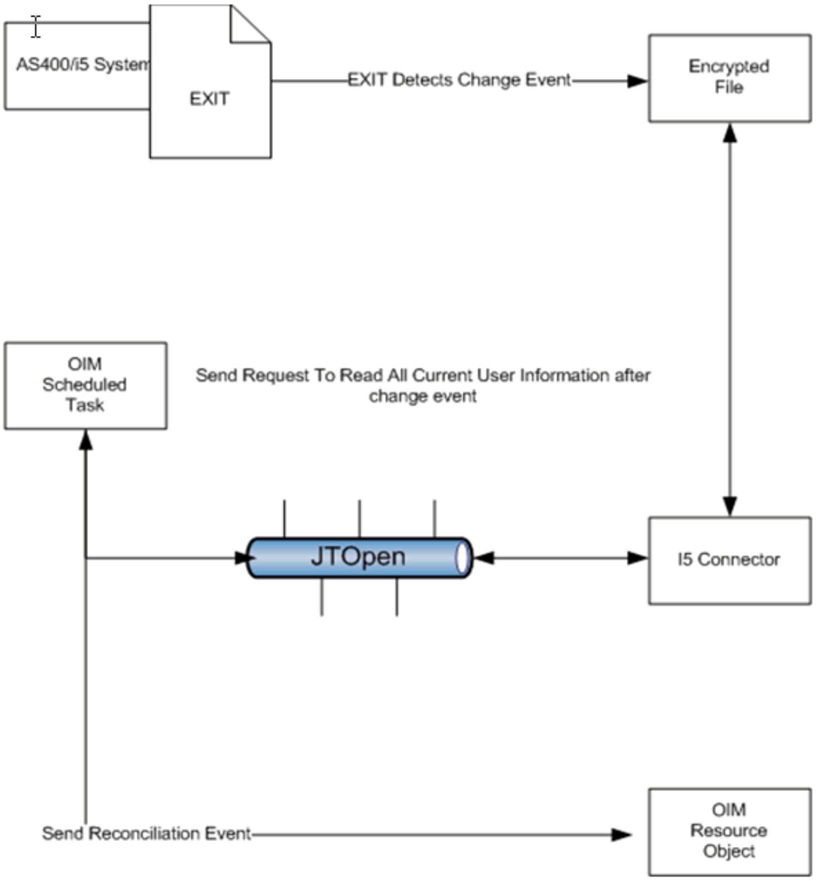
   > **Note:** Identity and authorization events in the IBM AS/400 system include the running of a command, real-time password synchronization, creation or deletion of a user, or a change in user data.

2. You specify a date/time timestamp in the OIM As400 IT Resource. The AS400 User Reconciliation scheduled task, using the LDAP Gateway, sends scheduled requests to the Provisioning Agent to search the target system for events made after the specified timestamp.
3. The Provisioning Agent encrypts user profile data for the events and then passes this data to the LDAP Gateway.
4. The LDAP Gateway decrypts the user profile data and passes it to Oracle Identity Manager.
5. The next step depends on the setting in the scheduled task:
   - If you configure the target system as a target resource, then the user profile data is converted into accounts or resources assigned for OIM Users.
   - If you configure the target system as a trusted source, then the user profile data is used to create OIM Users.

1.4.2.3 Incremental (Real-Time) Reconciliation Process

Real-time reconciliation is initiated by the EXIT(s) that work in conjunction with the Reconciliation Agent. See Figure 1–1.

Figure 1–1 Incremental (Real-Time) Reconciliation Process


AS400/i5 System
EXIT
EXIT Detects Change Event
Encrypted File
OIM Scheduled Task
Send Request To Read All Current User Information after change event
JTOpen
I5 Connector
Send Reconciliation Event
OIM Resource Object

1. IBM AS/400 identity and authorization events take place in the target system. After each event the EXIT will populate an encrypted file on the OS that contains all changed events.

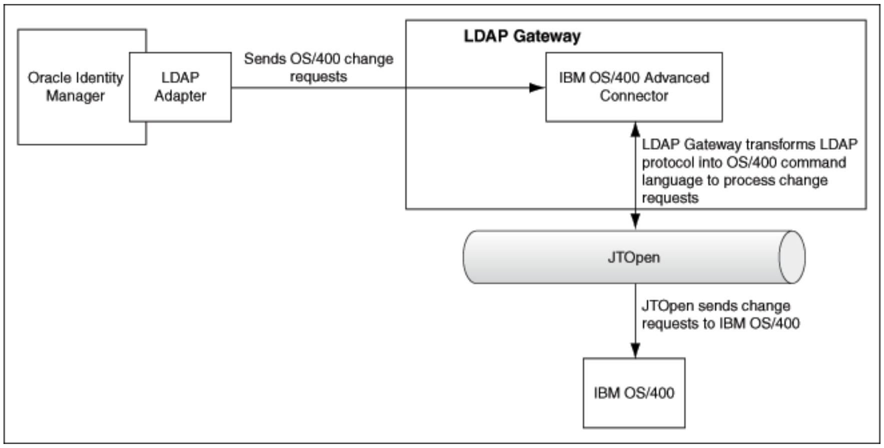
   Note: Identity and authorization events in the IBM AS/400 system include the running of a command, real-time password synchronization, creation or deletion of a user, or a change in user data.

2. To retrieve these events you run the newAS400 Reconcile All Changed Users scheduled task. This process will read the file and store the contents of event changes in an internally configured directory in the LDAP (based on the domainOu configuration). After the contents have been stored in the Internal LDAP the Task will query the internal store based on the Last Mod Timestamp in the OIM As400 IT Resource and reconcile any changes during that time to OIM.
3. The next step depends on the setting in the scheduled task:
   - If you configure the target system as a target resource, then the user profile data is converted into accounts or resources assigned for OIM Users.
   - If you configure the target system as a trusted source, then the user profile data is used to create OIM Users.

1.4.2.4 Provisioning Process

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

Figure 1–2 Provisioning Process


Oracle Identity Manager
LDAP Adapter
Sends OS/400 change requests
LDAP Gateway
IBM OS/400 Advanced Connector
LDAP Gateway transforms LDAP protocol into OS/400 command language to process change requests
JTOpen
JTOpen sends change requests to IBM OS/400
IBM OS/400

The following is a summary of the provisioning process:

1. Provisioning data submitted from the Administrative and User Console is sent to the LDAP Gateway.
2. The LDAP Gateway translates the provisioning data to IBM AS/400 commands.
3. The data is encrypted and then sent 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 AS/400 repository, and returns a success or error message to the LDAP Gateway.

1.5 Features of the Connector

This section discusses the following topics:

- Section 1.5.1, "Target Resource and Trusted Source Reconciliation"
- Section 1.5.2, "Full and Incremental Reconciliation"
- Section 1.5.3, "Encrypted Communication Between the Target System and Oracle Identity Manager"
- Section 1.5.4, "High Availability Feature of the Connector"

1.5.1 Target Resource and Trusted Source Reconciliation

You can use the connector to configure IBM AS/400 as either a target resource or trusted source of Oracle Identity Manager.

1.5.2 Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user profile data from the target system to Oracle Identity Manager.

Additionally, change-based or incremental reconciliation is available. Both forms of reconciliation are configured using the scheduled reconciliation task.

Section 4.1, "Configuring Reconciliation" describes the procedure.

You can perform a full reconciliation run at any time.

1.5.3 Encrypted Communication Between the Target System and Oracle Identity Manager

AES-128 encryption is used to encrypt data that is exchanged between the LDAP Gateway and the Provisioning Agent on the mainframe.

1.5.4 High Availability Feature of the Connector

If you have multiple installations of the target system, then you can configure one LDAP Gateway to work with each installation of the target system. Alternatively, you can configure a single LDAP Gateway installation to work with multiple installations of the target system. Section 5.5, "Configuring the Connector for Multiple Installations of the Target System" describes the procedure.

1.6 Connector Objects Used During Reconciliation and Provisioning

The following sections provide information about connector objects used during reconciliation and provisioning:

- Section 1.6.1, "Supported Functions for Target Resource and Trusted Source Reconciliation"
- Section 1.6.2, "Supported Functions for Provisioning"
- Section 1.6.3, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.4, "User Attributes for Trusted Source Reconciliation"
- Section 1.6.5, "Reconciliation Rule"
- Section 1.6.6, "Reconciliation Action Rules"

1.6.1 Supported Functions for Target Resource and Trusted Source Reconciliation

The connector supports reconciliation of user data from the following events:

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

1.6.2 Supported Functions for Provisioning

Table 1–2 lists the provisioning functions supported by the connector.

Table 1–2 Supported Provisioning Functions

Function	Description	Mainframe Command
Create users	Adds new users on IBM AS/400	CRTUSRPRF
Modify users	Modifies user data on IBM AS/400	CHGUSRPRF
Delete users	Removes users from IBM AS/400	DLTUSRPRF
Change passwords	Changes user passwords on IBM AS/400 in response to password changes made on Oracle Identity Manager through user self-service	CHGUSRPRF
Reset passwords	Resets user passwords on IBM AS/400 The passwords are reset by the administrator.	CHGUSRPRF
Revoking user accounts	Sets IBM AS/400 users to a REVOKED state	CHGUSRPRF
Resuming user accounts	Sets IBM AS/400 users to an ENABLED state	CHGUSRPRF

1.6.3 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 lists attribute mappings between IBM AS/400 and Oracle Identity Manager for target resource reconciliation and provisioning.

> **Note:** You can add new attributes for target resource reconciliation. Section 5.1, "Adding New Attributes for Target Resource Reconciliation" describes the procedure.

Table 1–3 User Attributes for Target Resource Reconciliation and Provisioning

Oracle Identity Manager Field	IBM AS/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	Owner of the user profile
status	STATUS	User status (enable, disable)
spcaut	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

1.6.4 User Attributes for Trusted Source Reconciliation

Table 1–4 lists attribute mappings between IBM AS/400 and Oracle Identity Manager for trusted source reconciliation.

Table 1–4 User Attributes for Trusted Source Reconciliation

OIM User Field	IBM AS/400 Attribute	Description
cn	NAME	Full name
uid	USER	Login ID
userPassword	PASSWORD	Password used to log in

1.6.5 Reconciliation Rule

> **See Also:** *Oracle Identity Manager Connector Concepts* for generic information about reconciliation matching and action rules

During target resource reconciliation, Oracle Identity Manager tries to match each user profile fetched from IBM AS/400 with existing IBM AS/400 resources provisioned to OIM Users. This is known as process matching. A reconciliation rule is applied for process matching. If a process match is found, then changes made to the user profile on the target system are copied to the resource on Oracle Identity Manager. If no match is found, then Oracle Identity Manager tries to match the user profile against existing OIM Users. This is known as entity matching. The reconciliation rule is again applied during this process. If an entity match is found, then an IBM AS/400 resource is provisioned to the OIM User. Data for the newly provisioned resource is copied from the user profile.

During trusted reconciliation, the same reconciliation rule is applied for entity matching. If an entity match is found, then an OIM User is created out of the data in the reconciliation event.

The following is the reconciliation rule for both target resource and trusted source reconciliation:

Rule name: AS400AdvReconRule

Rule element: User Login Equals uid

In this rule element:

- User Login is the User ID field on the process form and the OIM User form.
- uid is the USER attribute on IBM AS/400.

After you deploy the connector, you can view this reconciliation rule by performing the following steps:

1. On the Design Console, expand **Development Tools** and then double-click **Reconciliation Rules**.
2. Search for and open the **AS400AdvReconRule** rule.

1.6.6 Reconciliation Action Rules

Reconciliation action rules specify actions that must be taken depending on whether or not matching IBM AS/400 resources or OIM Users are found when the reconciliation rule is applied. Table 1–5 lists the reconciliation action rules for this connector.

Table 1–5 Reconciliation Action Rules

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rules for such rule conditions. See *Oracle Identity Manager Design Console Guide* for information about modifying or creating reconciliation action rules.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. On the Design Console, expand **Resource Management** and double-click **Resource Objects**.
2. Search for and open the **OIMAs400ResourceObject** resource object.
3. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector.

2

Connector Deployment on Oracle Identity Manager

The LDAP Gateway acts as the intermediary between Oracle Identity Manager and the connector components on the mainframe. The following sections of this chapter describe the procedure to deploy some components of the connector, including the LDAP Gateway, on the Oracle Identity Manager host computer:

> **Note:** The procedure to deploy the mainframe components of the connector is described in the next chapter.

- Section 2.1, "Files and Directories that Comprise the Connector"
- Section 2.2, "Determining the Release Number of the Connector"
- Section 2.3, "Before Running the Connector Installer"
- Section 2.4, "Running the Connector Installer"
- Section 2.5, "Configuring the IT Resource"
- Section 2.6, "Configuring Oracle Identity Manager"
- Section 2.7, "Configuring Trusted Source Reconciliation"
- Section 2.8, "Configuring Oracle Identity Manager for Request-Based Provisioning"
- Section 2.9, "Installing and Configuring the LDAP Gateway"

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
configuration/AS400Adv.xml	This XML file contains configuration information that is used during connector installation.
DataSets/ProvisionResource_OIMAS400ResourceObject.xml DataSets/ModifyResource_OIMAS400ResourceObject.xml	This XML file specifies the information to be submitted by the requester during a request-based provisioning operation. Section 2.8, "Configuring Oracle Identity Manager for Request-Based Provisioning" provides more information.
etc/LDAP Gateway/ldapgateway.zip	This ZIP file contains the files required to deploy the LDAP Gateway.

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

File or Directory on the Installation Media	Description
etc/Provisioning and Reconciliation Connector/OIMIDFEX.SAVF	This ZIP file contains the files required to deploy the Reconciliation Agent on the mainframe. Section 3.1, "Deploying the Reconciliation Agent" describes the files bundled in this ZIP file.
lib/as400-adv-provisioning.jar For Oracle Identity Manager release 11.1.1: lib-11G/as400-adv-provisioning.jar	This JAR file containing the files required for reconciliation and provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduledTask *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
Files in the resources directory	Each of these resource bundles contains locale-specific information that is used by the connector. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
For Oracle Identity Manager release 9.1.0.x: scripts/propertyEncrypt.bat scripts/propertyEncrypt.sh For Oracle Identity Manager release 11.1.1: scripts-11G/propertyEncrypt.bat scripts-11G/propertyEncrypt.	You use this script to encrypt passwords that you enter in the as400Connection.properties and beans.xml files. Section 2.9, "Installing and Configuring the LDAP Gateway" provides more information.
xml/oimAs400AdvConnector.xml	This XML file contains definitions of the connector components, such as the IT resource and resource object. These objects are created in Oracle Identity Manager when you import the XML file. Copy these XML files into the following directory: *OIM_HOME*/XLIntegrations/as400/xml/
xml/AS400TrustedXellerateUser.xml	This XML file contains definitions of the connector components that are used for trusted source reconciliation. Copy these XML files into the following directory: *OIM_HOME*/XLIntegrations/as400/xml/

2.2 Determining the Release Number of the Connector

> **Note:** If you are using Oracle Identity Manager release 9.1.0.*x*, then the procedure described in this section is optional.
>
> If you are using Oracle Identity Manager release 11.1.1, then skip this section.

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the connector JAR file that is in the *OIM_HOME*/xellerate/JavaTasks directory.
2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the connector JAR file.

   In the Manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.3 Before Running the Connector Installer

Prior to running the Connector Installer, you will need to delete the script and lib directories that do not pertain to your Oracle Identity Manager release version. If running Oracle Identity Manager release 9.1.x:

- Delete the "scripts-11G" directory from the connector package.
- Delete the "lib-11G" directory from the connector package.

If running Oracle Identity Manager release 11.1.1:

- Delete the "scripts" directory from the connector package.
- Delete the "lib" directory from the connector package.
- Rename the "scripts-11G" directory to "scripts".
- Rename the "lib-11G" directory to "lib".

2.4 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

   > **Note:** In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

   - For Oracle Identity Manager release 9.1.0.*x*:
     OIM_HOME/xellerate/ConnectorDefaultDirectory
   - For Oracle Identity Manager release 11.1.1:
     OIM_HOME/server/ConnectorDefaultDirectory
2. If you are using Oracle Identity Manager release 9.1.0.*x*, then delete the files that are meant for Oracle Identity Manager release 11.1.1. Similarly, if you are using

Oracle Identity Manager release 11.1.1, then delete the files that are meant for Oracle Identity Manager release 9.1.0.*x*. See Table 2–1 for information about files that are created for each Oracle Identity Manager release.

3. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide

   - For Oracle Identity Manager release 11.1.1:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.

   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.

5. From the Connector List list, select **IBM AS/400 Advanced *RELEASE_NUMBER***. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

   c. From the Connector List list, select **IBM AS/400 Advanced *RELEASE_NUMBER***.

6. Click **Load**.

7. To start the installation process, click **Continue**.

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see Section 2.7, "Configuring Trusted Source Reconciliation."

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.

8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

    a. Ensuring that the prerequisites for using the connector are addressed.

    > **Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.6.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.
    >
    > There are no prerequisites for some predefined connectors.

    b. Configuring the IT resource for the connector.

    Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

    c. Configuring the scheduled task that is created when you install the connector.

    > **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
    >
    > See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

    Record the names of the scheduled task that is displayed on this page. The procedure to configure this scheduled task is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Section 2.1, "Files and Directories that Comprise the Connector" for information about the files that you must copy and their destination locations on the Oracle Identity Manager host computer.

2.5 Configuring the IT Resource

You must specify values for the parameters of the As400Resource IT resource as follows:

1. Log in to the Administrative and User Console.

2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.

3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `As400Resource` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–2 describes each parameter.

Table 2–2 IT Resource Parameters

Parameter	Description
AtMap User	This parameter holds the 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	Set a user ID for an account that the connector will use to connect to the LDAP Gateway. Format: `cn=`*`USER_ID`*`,dc=as400,dc=com` Sample value: `cn=idfAs400Admin,dc=as400,dc=com` You also set this user ID in the beans.xml file inside the idfserver.jar file. See Step 7 in Section 2.9, "Installing and Configuring the LDAP Gateway."
idfPrincipalPwd	Set a password for the account that the connector will use to connect to the LDAP Gateway. You also set this password in the files listed in the description of the idfPrincipalDn parameter. **Note:** Do not enter an encrypted value.
idfRootContext	This parameter holds the root context for IBM AS/400. Value: `dc=as400,dc=com` **Note:** You must not change the value of this parameter.
idfServerHost	This parameter holds the host name of the computer on which you install the LDAP Gateway. For this release of the connector, you install the LDAP Gateway on the Oracle Identity Manager host computer. Value: `localhost` **Note:** You must not change the value of this parameter.
idfServerPort	Enter the number of the port for connecting to the LDAP Gateway. Sample value: `6389` You also set this port number in the beans.xml inside the idfserver.jar file. See Step 7 in Section 2.9, "Installing and Configuring the LDAP Gateway."

Table 2–2 (Cont.) IT Resource Parameters

Parameter	Description
Last Modified Time Stamp	The most recent start time of the reconciliation scheduled task is stored in this parameter. See Section 4.1, "Configuring Reconciliation" for more information about this scheduled task. The format of the value stored in this parameter is as follows: `MM/dd/yy hh:mm:ss a` In this format: ■ `MM` is the month of the year. ■ `dd` is the day of the month. ■ `yy` is the year. ■ `hh` is the hour in am/pm (01-12). ■ `mm` is the minute in the hour. ■ `ss` is the second in the minute. ■ a is the marker for AM or PM. Sample value: `05/07/10 02:46:52 PM` The default value is `0`. Full reconciliation is performed when the value is 0. If the value is a non-zero, standard time-stamp value in the format given above, then incremental reconciliation is performed. Only target system records that have been created or modified after the specified time stamp are brought to Oracle Identity Manager for reconciliation. **Note:** When required, you can manually enter a time-stamp value in the specified format.
idfSSL	This parameter determines whether the LDAP Gateway will use SSL to connect to the target system. Enter true if using SSL. Otherwise, enter false. Sample value: `true`
idfTrustStore	This parameter holds the directory location of the trust store containing the SSL certificate. This parameter is optional, and should only be entered when using SSL authentication. Sample value: `C:/software/ldapgateway/conf/idf.jks`
idfTrustStorePassword	This parameter holds the password for the SSL trust store. This parameter is optional, and should only be entered when using SSL authentication.
idfTrustStoreType	This parameter holds the trust store type for the SSL trust store. This parameter is optional, and should only be entered when using SSL authentication. Sample value: `jks`

8. To save the values, click **Update**.

2.6 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

- Section 2.6.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.6.2, "Enabling Logging"
- Section 2.6.3, "Copying the log4j JAR File"

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster.

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

Note: In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to 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, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/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:

   For Oracle Identity Manager release 9.1.0.*x*:

   ```
   OIM_HOME/xellerate/bin/SCRIPT_FILE_NAME
   ```

   For Oracle Identity Manager release 11.1.1:

   ```
   OIM_HOME/server/bin/SCRIPT_FILE_NAME
   ```

2. Enter one of the following commands:

   Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

   For example, the following commands purge Metadata entries from the server cache:

   ```
   PurgeCache.bat MetaData
   ```

   ```
   PurgeCache.sh MetaData
   ```

   - For Oracle Identity Manager release 9.1.0.*x*:

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 delete from the server cache. See the following file for information about the other content categories:

OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

  t3://*OIM_HOST_NAME*:*OIM_PORT_NUMBER*

  In this format:

  – Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.

  – Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.6.2 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:

- **IBM WebSphere Application Server**

  To enable logging:

  1. In the *OIM_HOME*/xellerate/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

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, locate or 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

- **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

- **Oracle 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 displayed on the server console.

2.6.3 Copying the log4j JAR File

This connector uses the log4j JAR file that you copy into the *OIM_DC_HOME*/xlclient/ext directory while installing the Oracle Identity Manager Design Console. If this JAR file is not present in the *OIM_DC_HOME*/xlclient/ext directory, then:

1. Locate the log4j JAR file in the directory in which you install the application server on which Oracle Identity Manager is running.
2. Copy log4j JAR file into the *OIM_DC_HOME*/xlclient/ext directory.
3. Restart the application server.

2.7 Configuring Trusted Source Reconciliation

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to configure IBM AS/400 as a trusted source for identity data. By performing this procedure, you enable trusted source reconciliation for both full reconciliation runs and incremental reconciliation.

The XML file for trusted source reconciliation, AS400TrustedXellerateUser.xml, contains definitions of the connector components that are used for trusted source reconciliation. To import this XML file:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation pane.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.

4. Locate and open the AS400TrustedXellerateUser.xml file from the xml directory on the installation media. 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**.

2.8 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

> **Note:** Direct provisioning allows the provisioning of multiple target system accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Section 2.8.1, "Copying Predefined Request Datasets"
- Section 2.8.2, "Importing Request Datasets into the MDS"
- Section 2.8.3, "Enabling the Auto Save Form Feature"
- Section 2.8.4, "Running the PurgeCache Utility"

2.8.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following predefined request datasets are available in the DataSets directory on the installation media:

ProvisionResource_OIMAS400ResourceObject.xml

ModifyResource_OIMAS400ResourceObject.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\as400Adv

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide* for Oracle Identity Manager for information on modifying request datasets.

2.8.2 Importing Request Datasets into the MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into the MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

   > **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.8.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\as400Adv directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

2. In a command window, change to the *OIM_HOME*\server\bin directory.

3. Run one of the following commands:

   - On Microsoft Windows

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

4. When prompted, enter the following values:

   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

- `Please enter your password [weblogic]`

  Enter the password used to log in to the WebLogic server.

- `Please enter your server URL [t3://localhost:7001]`

  Enter the URL of the application server in the following format:

  `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

  In this format, replace:

  - *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.
  - *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS at the following location:

/custom/connector/*RESOURCE_NAME*

2.8.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **OIMAS400AdvProvisioningProcess** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.8.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.6.1, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

2.9 Installing and Configuring the LDAP Gateway

The IT resource contains connection information for Oracle Identity Manager to connect to the LDAP Gateway. The as400.properties file is one of the components of the gateway. This file contains information used by the gateway to connect to the mainframe. Configuring the gateway involves setting values in the as400.properties file and the other files that are used by the 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. This ZIP file is in the etc/LDAP Gateway directory on the installation media.

   > **Note:** In this document, the full path (and name) of the ldapgateway directory on the Oracle Identity Manager host computer is referred to as *LDAP_INSTALL_DIR*.

2. Download JTOpen from the IBM Web site at

http://www14.software.ibm.com

3. Extract the contents of the jtopen_ver.zip file.

4. 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 Section 2.9, "Installing and Configuring the LDAP Gateway."

5. Open the *LDAP_INSTALL_DIR*/conf/as400.properties file in a text editor, and specify values for the properties described in Table 2–3.

Table 2–3 LDAP Gateway Properties in the as400.properties File

Property	Description	Sample Value
host	Set the host name or IP address of the IBM AS/400 host computer as the value of this property.	`127.0.0.1`
adminId	User ID of a target system administrator with SystemAdministrators privileges	`test`
adminPwd or _adminPwdEncrypt_	Password of the target system administrator with SystemAdministrators privileges If you do not encrypt the password, then use the _adminPwd_ property to enter the password. If you encrypt the password, then use the _adminPwdEncrypt_ property. See Step 7 of Section 2.9, "Installing and Configuring the LDAP Gateway" for information about using the propertyEncryt script to encrypt passwords.	`test`
agentHost	Target system IP address for the Reconciliation Agent host computer In most cases, this is the same as the value of the _host_ property.	`127.0.0.1`
agentAdminId	Target system Reconciliation Agent administrator ID In most cases, this is the same as the value of the _adminId_ property.	`test`
agentAdminPwd or _agentAdminPwdEncrypt_	Target system Reconciliation Agent administrator password If you do not encrypt the password, then use the _agentAdminPwd_ property to enter the password. If you encrypt the password, then use the _agentAdminPwdEncrypt_ property. See Step 7 of Section 2.9, "Installing and Configuring the LDAP Gateway" for information about using the propertyEncryt script to encrypt passwords. In most cases, the password that you enter is the same as the value of the _adminPwd_ or _adminPwdEncrypt_ property.	`test`
agentLib	Target system library in which the Reconciliation Agent files are located	`LSVALGAARD`
agentFile	Reconciliation Agent file on the target system	`QCSRC`
agentMember	Reconciliation Agent user with privileges to access the file specified as the value of the _agentFile_ property	`EUSRPWD`
agentport	Target system port allocated to the Reconciliation Agent	`5490`

Table 2–3 (Cont.) LDAP Gateway Properties in the as400.properties File

Property	Description	Sample Value
ignoreUsers	Enter a pipe-separated list of user IDs to ignore when retrieving user profiles from the target system.	`QUSER|QTMHHTTP|QTFTP|QTCP|`
ignoreGroups	Enter a pipe-separated list of group IDs to ignore when retrieving group profiles from the target system.	`QTIVUSER|QTIVROOT|QTIVOLI|QDESUSR|`
isSSL	Enter one of the following as the value of this property: ■ Set true as the value of this property if you want the LDAP Gateway to use SSL to connect to the target system ■ Set false as the value of this property if you want the LDAP Gateway to use a regular connection to the target system	
defaultDelete	Enter one of the following as the value of this property: ■ 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.	`delete`
internalEnt	Enter one of the following as the value of this property: ■ Set true as the value of this property if you want the LDAP Gateway to use the internal LDAP store. ■ Set false as the value of this property if you do not want the LDAP Gateway to use the internal LDAP store.	

6. Save and close the as400.properties file.
7. 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:

   - LDAP Gateway user credentials

     Use the beans.xml file to store the credentials of the account used by Oracle Identity Manager to connect to the LDAP Gateway. You also enter these credentials as parameters of the IT resource. During provisioning and reconciliation, the credentials passed through the IT resource are authenticated against the credentials stored in the beans.xml file. The LDAP Gateway exchanges data with the connector only after this authentication succeeds.

     You enter the credentials of the LDAP Gateway user in the following lines of the beans.xml file:

     ```
     <property name="adminUserDN" value="cn=idfAs400Admin,dc=as400,dc=com"/>
     <property name="adminUserPassword" value="idfAs400Pwd"/>
     ```

     In the first line, replace **`cn=idfAs400Admin,dc=as400,dc=com`** with the value that you enter for the idfPrincipalDn parameter of the IT resource. In the second line, replace **`idfAs400Pwd`** with the value that you enter for the idfPrincipalPwd parameter of the IT resource. Table 2–2, " IT Resource Parameters" describes both parameters. If you want to encrypt the password before you enter it in the beans.xml file, then:

Note: It is optional to encrypt the password that you set in the beans.xml file. However, it is recommended that you encrypt the password for security reasons.

You must enter the unencrypted password as the value of the idfPrincipalPwd IT resource parameter. This is regardless of whether you enter the encrypted password in the beans.xml file.

---

a. In a text editor, copy one of the following script files from the installation media into a temporary directory and then open the script file in a text editor:

   For Microsoft Windows:

   ```
   /scripts/propertyEncrypt.bat
   ```

   For UNIX:

   ```
   /scripts/propertyEncrypt.sh
   ```

b. Specify values for the following properties in the file:

   ```
   SET CLASSPATH=DIRECTORY_LOCATION\idfserver.jar
   ```

   Replace *DIRECTORY_LOCATION* with the full path of the directory into which you copied the idfserver.jar file while deploying the connector.

   For example:

   ```
   SET CLASSPATH=C:\software\ldapgateway\dist\idfserver.jar
   ```

   ```
   %JAVACMD%  %JVM_OPTS%  -cp %CLASSPATH%
   com.identityforge.idfserver.util.AESCipherUtil PLAINTEXT_PASSWORD
   ```

   Replace *PLAINTEXT_PASSWORD* with the password that you want to encrypt.

   For example:

   ```
   %JAVACMD%  %JVM_OPTS%  -cp %CLASSPATH%
   com.identityforge.idfserver.util.AESCipherUtil idfAS400Pwd
   ```

c. Save the changes made to the propertyEncrypt script.

d. Run the script.

   The script encrypts the password that you provide and displays it in the command window.

e. In the beans.xml file, search for the following string:

   ```
   <property name="adminUserPassword"
   ```

f. Replace the value of this property with the encrypted password.

   For example:

   ```
   <property name="adminUserPassword"
   value="468018DD1CDBE82E515EBF78A41C428E"/>
   ```

- Port used for communication between the LDAP Gateway and the mainframe LPAR on which you install the connector mainframe component

---

Note: The procedure to install the mainframe component of the connector is described in the next chapter.

As shown in the following line, the default value of the port property is `5389` in the beans.xml file. You can change this default value to any port of your choice.

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

- Configuration for provisioning and initial reconciliation

  If you want the connector to perform provisioning and initial reconciliation but not incremental (that is, real-time) reconciliation, then change the value of the following property from `true` to `false`:

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

  Leave the value of the agent property as `false` if you want the connector to perform incremental reconciliation.

8. To enable logging for the LDAP Gateway:

   a. Copy the log4j JAR file from the application server directory in which it is placed to the *LDAP_INSTALL_DIR*/lib directory.

   b. Extract the log4j.properties file from the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.

   c. Enter a log level as the value of the log4j.rootLogger variable. For example:

   ```
   log4j.rootLogger=ERROR, A1
   ```

   d. Save and close the file.

   When you use the connector, the `idfserver.log.0:` log file is generated in the *LDAP_INSTALL_DIR*/logs directory. This is the main log file.

9. To configure SSL in the LDAP Gateway:

   a. Edit the /ldapgateway/idfserver.jar beans.xml directory for the following:

   ```
   < bean id="sslChannelFactory"
   class="com.identityforge.idfserver.nio.ssl. SSLChannelFactory">
   <constructor-arg><value>false</value></constructor-arg>
   <constructor-arg><value>./conf/idf.jks</value></constructor-arg>
   <constructor-arg><value>abc123</value></constructor-arg>
   <constructor-arg><value>false</value></constructor-arg>
   </bean >
   ```
   The first argument indicates we are not in client mode.

   Note: Do not change this argument.

   The second argument is the path to the keystore. Either change this path to your keystore or add your certificate to this keystore.

   The third argument is the keystore password that you used to generate your keystore.

   The fourth argument is whether the keystore password is encrypted.

b. Edit a listener using the SSLChannelFactory for only "port", which is the only item you can change in the listener:

```
<bean id="sslListener" class="com.identityforge.idfserver.nio.Listener">
constructor-arg><ref bean="bus"/></constructor-arg>
<constructor-arg><ref bean="sslChannelFactory"/></constructor-arg>
<property name="admin"><value>false</value></property>
<property name="config"><value>./conf/listener.xml</value></property>
<property name="port" value="7389"/>
<property name="threadName" value="SSLLDAPListener"/>
</bean>
```

c. Add the listener to the server by uncommenting the following line:

```
<bean id="server" class="com.identityforge.idfserver.Server">
<property name="tasks">
<list>
<ref bean="bus"/>
<ref bean="decoder"/>
<ref bean="listener"/>
<!-- <ref bean="sslListener"/> ? <!-- added here -->
<ref bean="client"/>
<ref bean="protocol"/>
<ref bean="encoder"/>
<ref bean="output"/>
</list>
</property>
<property name="nexus" ref="nexus"/>
<property name="logPath" value="../logs/idfserver.log"/>
</bean>
```

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

10. In a text editor, open the script, run.sh or run.bat file from the *LDAP_INSTALL_DIR*/bin directory.

11. In the run script, 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 instructions given in this step apply to Oracle Identity Manager release 9.1.0.*x*. For Oracle Identity Manager release 11.1.1, follow the instructions given in the run script itself.

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
```

12. 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
  ```

13. 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 script 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
    ```

14. Save and close the run script.

Starting and Stopping the LDAP Gateway on UNIX

To start the LDAP Gateway on UNIX, run the following command:

bin> ./run.sh

When the LDAP Gateway has started, the `LDAP Gateway` *`VERSION_NUMBER`* `Started` message is recorded in the in the *LDAP_INSTALL_DIR*/bin/nohup.out file.

To stop the LDAP Gateway on UNIX, run the following command:

bin> ./stop_idf.sh

Starting and Stopping the LDAP Gateway on Microsoft Windows

To start the LDAP Gateway on Microsoft Windows, run the run.bat file.

When the LDAP Gateway has started, the `LDAP Gateway` *`VERSION_NUMBER`* `Started` message is recorded in the in the service log.

To stop the LDAP Gateway on Microsoft Windows, close the command window in which the gateway is running.

3

Connector Deployment on the iSeries

You deploy the Reconciliation Agent on the mainframe. The following sections describe the installation and configuration of the Reconciliation Agent and the exits used by the agent:

- Section 3.1, "Deploying the Reconciliation Agent"
- Section 3.2, "Installing the Exits for the Reconciliation Agent"
- Section 3.3, "Configuring the Message Transport Layer"

3.1 Deploying the Reconciliation Agent

To deploy the Reconciliation Agent:

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

   > **Note:** In this guide, the directory to which the OIMIDFEX.SAVF file is transmitted is referred to as LSVALGAARD.

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

   ```
   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 of 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 accepts 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 accepts the directory name and file name of the savefile.
   - The RSTLIB parameter accepts the new library in which you restore the savefile 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 AS/400 that can be used by the system or a user.

3.2 Installing the Exits for the Reconciliation Agent

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 a menu-driven protocol.

1. Log in to the IBM AS/400 system as a system administrator.
2. Ensure that the connector library files and objects are present in the LSVALGAARD directory. See the preceding section for more information.
3. Start the WRKREGINF User Exit Registration program, as shown:

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

   In IBM AS/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 registering the new version.
4. You must register the exit points that are required for the Reconciliation Agent with IBM AS/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 AS/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 block, QGLDPUEXIT represents this exit point in the main system library QSYS, which implies that the IBM AS/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 press 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:

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

```
            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
```

8. Enter the WRKSYSVAL command, and then 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 AS/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 AS/400 Advanced connector is designed for and has been tested on level 50.

3.3 Configuring the Message Transport Layer

To configure the message transport layer on the IBM AS/400 system, you configure the NOTIFY exit IP address as follows:

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 host computer IP address, 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 6 character positions, with leading zeros in the number. A colon (:) is in the seventh character position. The IP address starts at the eighth 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 AS/400 does not require an IPL.

4 Using the Connector

This chapter discusses the following topics:

- Section 4.1, "Configuring Reconciliation"
- Section 4.2, "Configuring Account Status Reconciliation"
- Section 4.3, "Guidelines on Using the Connector"
- Section 4.4, "Performing Provisioning Operations"
- Section 4.5, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"

4.1 Configuring Reconciliation

The AS400 User Reconciliation scheduled task scheduled task performs both full

and incremental reconciliation. When you configure this scheduled task, it runs at specified intervals and fetches create, delete, or modify events on the target system for reconciliation.

To configure the AS400 User Reconciliation scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Perform one of the following steps:
   a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**

   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

     a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

     b. In the search results table, click the edit icon in the Edit column for the scheduled task.

     c. On the Scheduled Task Details page, where the details of the scheduled task that you selected are displayed, click **Edit**.
   - If you are using Oracle Identity Manager release 11.1.1, then:

   a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

   b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

   c. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. Modify the details of the scheduled task. To do so:

   a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

      – **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

      – **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.

      – **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

      – **Frequency:** Specify the frequency at which you want the task to run.

   b. If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, you can modify the following parameters:

      – **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

      – **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

   Note: See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

   In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task. To do so:

   Note:

   - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
   - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

Table 4–1 describes the attributes of the scheduled task.

Table 4–1 Attributes of the User Target Recon Scheduled Task Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `As400Resource`
Resource Object	Enter the name of the resource object against which reconciliation runs must be performed. Sample value: `OIMAs400AdvResourceObject`
Trusted Resource Object	Enter the name of the resource object against which trusted reconciliation runs must be performed. Sample value: `Xellerate User`
MultiValueAttributes	Enter a comma-separated list of multi-valued attributes that you want to reconcile. Do not include a space after each comma. Sample value: `spcaut,supgrpprf`
SingleValueAttributes	Enter a comma-separated list of single-valued attributes that you want to reconcile. Do not include a space after each comma. Do not include attributes already listed in the MultiValueAttributes field. Sample value: `uid,owner,text,usrcls,inlmnu,cn,inlpgm`
TrustedReconciliation	Enter whether the target system should be treated as a trusted source. Sample value: `true`
LDAP Time Zone	Enter the time zone ID for the server on which the LDAP gateway is hosted. Sample value: `America/New_York`
UsersList	Enter a comma-separated list of user IDs to be reconciled. **Note**: This field is optional. If no user IDs are listed, and the "Last Modified Time Stamp" (LMTS) attribute on the As400 IT Resource is '0', then full reconciliation will be performed. If no user IDs are listed, and the LMTS attribute on the As400 IT Resource is a date/time value, then only users modified after the LMTS will be reconciled. If user IDs are listed, and the LMTS is "0", then only the listed user IDs will be reconciled. If users IDs are listed, and the LMTS is a date/time value, then only listed user IDs that have been modified since the LMTS will be reconciled. Sample value: `testusr1,testusr2,testusr3`

6. After specifying the attributes, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

> **Note:** The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console. See the "The Task Scheduler Form" section in *Oracle Identity Manager Design Console Guide* for information about this feature.

- If you are using Oracle Identity Manager release 11.1.1, then click **Apply** to save the changes.

> **Note:** The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

4.2 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 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 OIMAS400AdvProvisioningProcess process definition, map the field for the status attribute to the OIM_OBJECT_STATUS field.
   - In the OIM User Recon Scheduled Task, add the status attribute's name to the list of attributes in the SingleValueAttribute section.

4.3 Guidelines on Using the Connector

Apply the following guidelines while using the IBM AS/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, 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 AS/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.
- Reconciliation data for the following fields might look different from provisioning data for the same fields:
  - Initial Program (INLPGM)
  - Initial Menu (INLMNU)
  - Job Description (JOBD)

The reconciliation data displays the expanded value, which includes the path qualifiers. For example, /QSYS.LIB/%LIBL%.LIB/MAIN.MNU. During provisioning, the connector accepts values for these fields without path qualifiers. If you do not include path qualifiers during provisioning, then IBM AS/400 adds the path qualifiers.

4.4 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 4.5, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

This following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

> **See Also:** *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

- Section 4.4.1, "Direct Provisioning"
- Section 4.4.2, "Request-Based Provisioning"

4.4.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.
     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.

3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. From the Users menu, select **Manage**.
     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the user details page, click the **Resources** tab.
     b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
5. On the Step 1: Select a Resource page, select **OIMAs400ResourceObject** from the list and then click **Continue**.
6. On the Step 2: Verify Resource Selection page, click **Continue**.
7. On the Step 5: Provide Process Data for AS400 Advanced Details page, enter the details of the account that you want to create on the target system and then click **Continue**.
8. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
9. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. Close the window displaying the "Provisioning has been initiated" message.
     b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

4.4.2 Request-Based Provisioning

> **Note:** The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

> **Note:** The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 4.4.2.1, "End User's Role in Request-Based Provisioning"
- Section 4.4.2.2, "Approver's Role in Request-Based Provisioning"

4.4.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **OIMAs400ResourceObject**, move it to the Selected Resources list, and then click **Next**.

11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.

    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

4.4.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

4.5 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

> **Note:** It is assumed that you have performed the procedure described in Section 2.8, "Configuring Oracle Identity Manager for Request-Based Provisioning."

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:

   a. Expand **Process Management**, and then double-click **Process Definition**.

   b. Search for and open the **OIMAS400AdvProvisioningProcess** process definition.

   c. Deselect the Auto Save Form check box.

   d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:

   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **OIMAs400ResourceObject** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **OIMAS400AdvProvisioningProcess** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.
3. If you want to enable end users to raise requests for themselves, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **OIMAs400ResourceObject** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the Save icon.

5

Extending the Functionality of the Connector

The following are optional procedures that you can perform to extend the functionality of the connector for addressing your business requirements:

- Section 5.1, "Adding New Attributes for Target Resource Reconciliation"
- Section 5.2, "Adding New Attributes for Provisioning"
- Section 5.3, "Removing Attributes Mapped for Target Resource Reconciliation and Provisioning"
- Section 5.4, "Using the Additional Reconciliation Scheduled Tasks"
- Section 5.5, "Configuring the Connector for Multiple Installations of the Target System"

5.1 Adding New Attributes for Target Resource Reconciliation

> **Note:** You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in Table 1–3 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

To add a new attribute for target resource reconciliation:

1. The SingleValueAttributes and MultiValue Attributes properties of the AS400 User Reconciliation scheduled task contain the list of target system attributes that are mapped for reconciliation with Oracle Identity Manager. If you want to add an attribute for reconciliation, then add it to the list of attributes in the appropriate section.
2. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:
   a. Open the Resource Objects form. This form is in the Resource Management folder.
   b. Click **Query for Records**.
   c. On the Resource Objects Table tab, double-click the **OIMAs400ResourceObject** resource object to open it for editing.

d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.

e. Specify a value for the field name.

   You must specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 1.

f. From the **Field Type** list, select a data type for the field.

   For example: `String`

g. Save the values that you enter, and then close the dialog box.

h. If required, repeat Steps d through g to map more fields.

i. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

3. If a corresponding field does not exist in the process form, then add a new column in the process form.

   a. Expand **Development Tools**.

   b. Double-click **Form Designer.**

   c. Search for and open the **UD_AS400ADV** process form.

   d. Click **Create New Version**, and then click **Add**.

   e. Enter the details of the field.

   f. Click **Save** and then click **Make Version Active.**

4. Modify the process definition to include the mapping between the newly added attribute and the corresponding reconciliation field:

   a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.

   b. Click the **Query for Records** icon.

   c. On the Process Definition Table tab, double-click the **OIMAS400AdvProvisioningProcess** process definition.

   d. On the Reconciliation Field Mappings tab, click **Add Field Map** to open the Add Reconciliation Field Mapping dialog box.

   e. From the **Field Name** list, select the name of the resource object that you add in Step 2.e.

   f. Double-click **Process Data Field** and select the corresponding process form field from the Lookup dialog box. Then, click **OK.**

   g. Click **Save** and close the dialog box.

5.2 Adding New Attributes for Provisioning

By default, the attributes listed in Table 1–3 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Log in to the Design Console.
2. Add the new attribute (field) on the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer.**
   c. Search for and open the **UD_AS400ADV** process form.
   d. Click **Create New Version**, and then click **Add**.
   e. Enter the details of the field.
   f. Click **Save** and then click **Make Version Active.**
3. To enable update of the attribute during provisioning operations, create a process task as follows:

   > **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

   a. Expand **Process Management**, and double-click **Process Definition**.
   b. Search for and open the **OIMAS400AdvProvisioningProcess** process definition.
   c. Click **Add**.
   d. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

      Conditional

      Required for Completion

      Allow Cancellation while Pending

      Allow Multiple Instances
   e. Click **Save**.
   f. On the Integration tab of the Creating New Task dialog box, click **Add**.
   g. In the Handler Selection dialog box, select **Adapter**, click **adpMODIFYUSER**, and then click the Save icon.

      The list of adapter variables is displayed on the Integration tab. The following screenshot shows the list of adapter variables:
   h. To create the mapping for the first adapter variable:

      Double-click the number of the first row.

      In the Edit Data Mapping for Variable dialog box, enter the following values:

      Variable Name: Adapter return value

      Map To: Process Data

      Qualifier: Return status

      Click the Save icon.

i. To create mappings for the remaining adapter variables, use the data given in the following table:

Variable Number	Variable Name	Map To	Qualifier
Second	idfResource	IT Resource	Not applicable
Third	uid	Process Data	LoginId
Fourth	attrName	Literal	`cn` string
Fifth	attrValue	Process Data	`UD_AS400_`*`NAME`* string

j. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

k. Click the Save icon to save changes to the process definition.

5.3 Removing Attributes Mapped for Target Resource Reconciliation and Provisioning

Note: You must not remove the uid, cn, password, or defaultGroup attribute. These attributes are mandatory on the target system.

The SingleValueAttributes and MultiValueAttributes sections of the User Recon Scheduled Task contain the list of target system attributes that are mapped for reconciliation. If you want to remove an attribute mapped for reconciliation, then remove it from the list in the appropriate section.

5.4 Using the Additional Reconciliation Scheduled Tasks

In addition to the standard AS400 User Reconciliation scheduled task, the connector also includes additional tasks to assist in user reconciliation. Table 5–1 describes each of the scheduled tasks and the properties they utilize.

Table 5–1 Scheduled Tasks and Properties

Scheduled Task	Description	Can utilize Last Modified Time Stamp	Requires LDAP Time Zone	Can utilize Users List	Requires Domain OU	Requires Store Internal (users are reconciled to internal LDAP store)
AS400 User Reconciliation	This task reconciles user profiles by retrieving a list of users from the target system, querying the target system for the profile of each user, and reconciling that user to Oracle Identity Manager.	X	X	X		
AS400 Single Connection User Reconciliation	This task reconciles user profiles by retrieving a list containing both users IDs and their profiles from the target system and stores those profiles in the internal LDAP store if needed. Then, all retrieved users are reconciled to Oracle Identity Manager.	X	X		X	X
AS400 Reconcile All Changed Users	This task reconciles user profiles by retrieving a list of modified users from an encrypted file on the target operating system, then querying the target system for the updated user profiles, and reconciling those profiles to Oracle Identity Manager.	X	X		X	

Table 5–1 (Cont.) Scheduled Tasks and Properties

Scheduled Task	Description	Can utilize Last Modified Time Stamp	Requires LDAP Time Zone	Can utilize Users List	Requires Domain OU	Requires Store Internal (users are reconciled to internal LDAP store)
AS400 Delete User Reconciliation Using LDAP	This task reconciles deleted users from the target system to the internal LDAP store and Oracle Identity Manager. Any user profiles that exist within the internal LDAP store, but not on the target system, are updated in the internal LDAP store and deleted from Oracle Identity Manager.		X	X	X	X
AS400 Delete User Reconciliation Using Oracle Identity Manager	This task reconciles deleted users from the target system to Oracle Identity Manager. Any user profiles that exist within Oracle Identity Manager, but not on the target system, are deleted from Oracle Identity Manager.		X	X	X	

5.5 Configuring the Connector for Multiple Installations of the Target System

Depending on your requirements, you can apply one of the following approaches to configure the connector for multiple installations of the target system:

- Section 5.5.1, "Configuring One LDAP Gateway for Each Installation of the Target System"
- 5.5.2 , "Configuring the LDAP Gateway to Work with Multiple Installations of the Target System"

5.5.1 Configuring One LDAP Gateway for Each Installation 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 that is configured to communicate with a single 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
   - Section 2.5, "Configuring the IT Resource" 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. 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 AS/400 running on each server.

5.5.2 Configuring the LDAP Gateway to Work with Multiple Installations of the Target System

You can configure a single LDAP Gateway installation to work with multiple installations of the target system. This is an alternative to setting up one LDAP Gateway for each target system installation.

To configure the LDAP Gateway to work with a second installation of the target system:

> **Note:** Repeat this procedure for each installation of the target system.

1. Create a directory inside the *LDAP_INSTALL_DIR* directory.
2. Create a copy of the existing as400.properties file, and place the copy inside the newly created directory.
3. Open the newly created properties file, and set values for the _host_ and _port_ properties so that they match the values of the LPAR/Provisioning Agent on the second installation of the target system.
4. Extract the contents of the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.
5. Open the beans.xml file in a text editor. This XML file is bundled in the idfserver.jar file.
6. In the beans.xml file, create a second instance of the <beans name=As400> element by copying and pasting it in the file itself.
7. In the newly copied element, change the value of the element from `As400` to some other string. For example: `<beans name=As400LPAR2>`
8. In the newly copied element, edit the properties that are shown in bold font in the following sample code block:

```
<bean name=" As400LPAR2" singleton="true"
class="com.identityforge.idfserver.backend.as400.AS400Module">
        <property name="suffix" value="dc=as400,dc=com"/>
        <property name="workingDirectory" value="../as4002"/>
        <property name="adminUserDN" value="cn=idfAs400Admin,
dc=as400,dc=com"/>
        <property name="adminUserPassword" value="idfAs400Pwd"/>
        <property name="allowAnonymous" value="true"/>
        <property name="entryCacheSize" value="1000"/>
        <property name="defaultUacc" value="read"/>
        <property name="searchUsersType" value="user"/>

        <property name="schema" ref="schemas"/>
        <property name="metaBackend"><ref bean="hpbe2"/></property>

        <property name="configLocation" value="../conf/as4002.properties"/>

        <property name="agent" value="false"/>
        <property name="agentAdapters">
            <list>
                <value> </value>
            </list>
        </property>
    </bean>
```

9. As shown in bold font in the following example, add an entry for each new <bean name= . . . > element in the NEXUS bean element for processing commands:

```
<property name="backends">
    <list>
        <ref bean="hpbe2"/>
        <!-- <ref bean="racf"/> -->
```

```
            <!-- <ref bean="tops"/> -->
            <!-- <ref bean="acf2"/> -->
            <ref bean="as400"/>
            <ref bean="as400LPAR2"/>
        </list>
    </property>
```

10. Save the beans.xml file, and then re-create the idfserver.jar.

> **Note:** If you configure the connector for trusted source reconciliation, then it must be set to `true` on all installations that connect to the same LDAP Gateway. Otherwise, the connector will fail.

6

Troubleshooting

Table 6–1 lists solutions to some commonly encountered issues associated with the connector.

Table 6–1 Troubleshooting

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the IBM AS/400 Server.	■ Ensure that the IBM AS/400 server is 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 AS/400 platform manager to verify that AS/400 user account and password have not been changed.
IBM AS/400 does not appear to respond.	■ Ensure that the Oracle Identity Manager attribute mappings are correct. ■ Check the configuration mappings for the LDAP 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 the connector. ■ If the event does not register in either of these two logs, investigate the connection between Oracle Identity Manager and the LDAP Gateway. ■ If the event is in the log but the command has not had the intended change on an IBM AS/400 user profile, check the configuration and connections between the LDAP Gateway and IBM AS/400.

7

Known Issues

There are no known issues associated with this release of the connector.

Index