Oracle® Identity Manager

Connector Guide for AS400

Release 11.1.1

E20671-13

February 2018

ORACLE

Oracle Identity Manager Connector Guide for AS400, Release 11.1.1

E20671-13

Primary Author: Gowri.G.R

Contributing Author: Prakash Hulikere, Nagesh Korlapati, Mahesh Nagaraj

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

5 Troubleshooting

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with an AS400 target system.

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 that have purchased support 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, vist the following Oracle Help Center page:

http://docs.oracle.com/cd/E52734_01/index.html

For information about Oracle Identity Manager Connectors documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E22999_01/index.htm

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.

Convention	Meaning
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 Oracle Identity Manager Connector for AS400?

This chapter provides an overview of the updates made to the software and documentation for the AS400 connector in release 11.1.1.6.0.

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

- Software Updates

  This section describes updates made to the connector software.

- 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:

- Software Updates in Release 11.1.1.6.0
- Software Updates in Release 11.1.1.5.0

Software Updates in Release 11.1.1.6.0

The following are issues resolved in release 11.1.1.6.0:

Bug Number	Issue	Resolution
16538788	Entitlement, IT resource, Account Name, and Account ID tagging were missing in the process form fields in Oracle Identity Manager 11.1.2.	This issue has been resolved.
16498811	The version of JTOpen 7.9 was not supported by the connector.	This issue has been resolved.
16496747	When a user was revoked from Oracle Identity Manager, the message queue associated with the user was not removed from AS400 target system. The revoke operation only removed the user profile.	This issue has been resolved.
16495891	User expiration date could not be provisioned or reconciled.	This issue has been resolved.

Software Updates in Release 11.1.1.5.0

This is the first release of the Oracle Identity Manager Connector for AS400 based on Identity Connector Framework (ICF). The following are software updates in release 11.1.1.5.0:

- ICF Based Connector
- Simplified Installation
- Deployment Using Connector Server
- New User Attributes
- New Lookup Definitions, Form Fields, and Scheduled Tasks
- New Resource Objects
- New Connector Operations
- New Data Validation

ICF Based Connector

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager and Oracle Waveset connectors require.

The Oracle Identity Manager Connector for AS400 is an ICF-based connector. The ICF uses classpath isolation, which allows the AS400 connector to co-exist with legacy versions of the connector.

For more information about the ICF, see Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

Simplified Installation

This release of the connector has a simplified installation process compared to previous releases. The AS400 connector no longer requires an LDAP Gateway. See Chapter 2, "Deploying the Connector" for more information.

Deployment Using Connector Server

This release of the connector can be deployed using the Connector Server, which is included with the ICF. See Section 2.1, "AS400 Connector Deployment Architecture With the Connector Server." for more information.

New User Attributes

This release of the connector has an extended set of user attributes. Some attributes are stored in an OS/400 Directory Entry object. Directory Entries were not used by previous releases of the connector. See Section 1.5.1, "User Attributes for Target Resource Reconciliation and Provisioning." for more information.

You can add to the standard set of attributes for reconciliation and provisioning. See Chapter 4, "Extending the Functionality of the Connector" for more information.

New Lookup Definitions, Form Fields, and Scheduled Tasks

This release of the connector has new Lookup definitions, Form Fields, and Scheduled Jobs. See the following topics for more information:

- Section 1.6, "Lookup Definitions Used During Connector Operations."

- Section 1.5.2, "Process Form Fields Used for Target Provisioning and Reconciliation"
- Chapter 3, "Using the Connector"

New Resource Objects

This release of the connector has new Resource Objects: AS400 User and AS400 Trusted User. See Section 1.7, "Resource Objects Used for Provisioning and Reconciliation." for more information.

New Connector Operations

This release of the connector supports before and after actions using scripts written in the OS/400 Command Language. See Section 3.4, "Configuring Action Scripts." and Section 2.2.2.1, "Creating a Target System User Account for AS400 Connector Operations" for more information.

New Data Validation

You can now configure validation for provisioned and reconciled single-valued data according to your requirements. See Section 4.2, "Configuring Validation and Transformation" for more information.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 11.1.1.6.0
- Documentation-Specific Updates in Release 11.1.1.5.0

Documentation-Specific Updates in Release 11.1.1.6.0

The following is a documentation-specific update in revision "13" of release 11.1.1.6.0:

- The "Target systems" row of Table 1–1, " Certified Components" has been updated.

The following is a documentation-specific update in revision "12" of release 11.1.1.6.0:

- The "Oracle Manager" row of Table 1–1, " Certified Components" has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12c (12.2.1.3.0) certification.

The following is a documentation-specific update in revision "11" of release 11.1.1.6.0:

- The "JDK" row of Table 1–1, " Certified Components" has been renamed to "Connector Server JDK".

The following are documentation-specific updates in revision "10" of release 11.1.1.6.0:

- A "Note" regarding trusted source IT resource has been added at the beginning of Section 2.4.8, "Configuring the IT Resource."
- The "JDK" row of Table 1–1, " Certified Components" has been updated.
- The "Connector Server" row has been added to Table 1–1, " Certified Components".

The following is a documentation-specific update in revision "9" of release 11.1.1.6.0:

Section 2.6, "Postcloning Steps" has been added.

The following are documentation-specific updates in revision "8" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of Table 1–1, " Certified Components" has been updated.

- Information specific to Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) has been added to Section 1.2, "Usage Recommendation."

The following is a documentation-specific update in revision "7" of release 11.1.1.6.0:

A "Note" regarding lookup queries has been added at the beginning of Chapter 4, "Extending the Functionality of the Connector."

The following is a documentation-specific update in revision "6" of release 11.1.1.6.0:

Information about limited reconciliation has been modified in Section 3.2.1, "Limited Reconciliation."

The following are documentation-specific updates in this release:

- The "Oracle Identity Manager" row of Table 1–1, " Certified Components" has been modified.
- A note has been added in the "datasets" and "xml" rows of Table 2–1, " Files and Directories On the Installation Media".
- The following sections have been added:
  - Section 2.4.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
  - Section 2.4.2, "Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later"
  - Section 2.4.11, "Localizing Field Labels in UI Forms"
  - Section 3.5, "Configuring Provisioning in Oracle Identity Manager Release 11.1.1"
  - Section 3.6, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Section 2.3.1, "Installing the AS400 Connector in Oracle Identity Manager"
  - Section 2.4.8, "Configuring the IT Resource"
  - Section 2.4.10, "Creating the IT Resource for the Connector Server"
  - Chapter 3.3, "Configuring Scheduled Jobs"

Documentation-Specific Updates in Release 11.1.1.5.0

The following documentation-specific update has been made in the revision "2" of the release 11.1.1.5.0:

- In Section 3.2.1, "Limited Reconciliation," the syntax of the Filter parameter has been changed.

The following documentation-specific update has been made in the revision "3" of the release 11.1.1.5.0:

- Section 2.3, "Installation" includes connector installation scenarios depending on where you want to run the connector code (bundle), either locally in Oracle Identity Manager or remotely in a Connector Server.

The following documentation-specific update has been made in the revision "4" of the release 11.1.1.5.0:

- In Section 2.4.7, "Enabling Logging," the logger name has been corrected.

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 documents the connector that enables you to use an IBM AS400 system as a managed (target) resource of Oracle Identity Manager.

Note: At some places in this guide, the term target system is used to refer to AS400, also known as OS/400, i5/OS, and IBM i.

In the account management (target resource) mode of the connector, data about users created or modified directly on the target system can be reconciled into Oracle Identity Manager. This data is used to provision (allocate) new resources or update resources already assigned to OIM users.

In addition, you can use Oracle Identity Manager to provision or update AS400 resources (that is, accounts) assigned to OIM users. These provisioning operations performed on Oracle Identity Manager translate into the creation of or updates to target system accounts.

This chapter contains the following sections:

1.1 Certified Components

Table 1–1 lists certified components for the AS400 connector.

Table 1–1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager: ■ Oracle Identity Governance 12c (12.2.1.3.0) ■ Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) and any later BP in this release track ■ Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) and any later BP in this release track ■ Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)
Target systems	AS400 (also known as OS/400, i5/OS, and IBM i) v5r4, IBM i 6.1, IBM i 7.1, IBM i 7.2, and IBM i 7.3
Connector Server	11.1.2.1.0
Connector Server JDK	JDK 1.6 or later
External code	JTOpen library version 6.2

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 9.1.0.1 or later and earlier than Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0), then you must use the 9.0.4 version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.0) or later, Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later, or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.*x* version of this connector.

1.3 Certified Languages

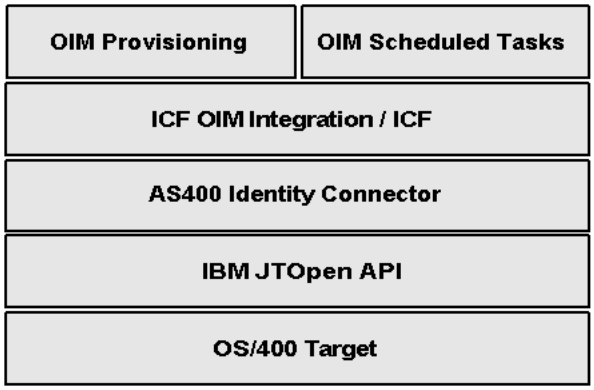
The AS400 connector supports the following languages:

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

1.4 Connector Architecture

The following figure shows the architecture for the AS400 connector.

Figure 1–1 Connector Architecture



Managing accounts consists of the following processes:

- Provisioning

  Provisioning involves creating or updating users on the target system through Oracle Identity Manager. When you allocate (or provision) a AS400 resource to an OIM User, the operation results in the creation of an AS400 user profile for that user. In the Oracle Identity Manager context, the term provisioning also covers updates made to the target system account through Oracle Identity Manager.

- Target resource reconciliation

  In target resource reconciliation, data related to newly created and modified target system accounts can be reconciled and linked with existing OIM users and provisioned resources. A scheduled job is used for reconciliation.

AS400 is configured as a target, or a trusted resource of Oracle Identity Manager. Through provisioning operations performed on Oracle Identity Manager, accounts are created and updated on the target system for OIM users. Through reconciliation, account data that is created and updated directly on the target system is fetched into Oracle Identity Manager and stored against the corresponding OIM users.

The AS400 connector is implemented using the Identity Connector Framework (ICF). The ICF provides a container that separates the connector bundle from the application. The ICF also provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering.

For more information about the ICF, see Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

1.5 Features of the Connector

The following are features of the AS400 connector:

- Section 1.5.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.5.3, "Reconciliation"

- Section 1.5.4, "Full or Incremental Reconciliation"
- Section 1.5.4.1, "Delete Reconciliation"
- Section 1.5.4.2, "Lookup Reconciliation"
- Chapter 1.5.5, "Support for Reconciliation of Account Status"
- Section 1.5.6, "Features Provided by the Identity Connector Framework"
- Section 1.5.7, "Support for Scheduled Tasks"
- Section 1.5.8, "Connection Pooling"
- Section 1.5.9, "Support for the Connector Server"

1.5.1 User Attributes for Target Resource Reconciliation and Provisioning

You can create mappings for attributes that are not included in the list of default attribute mappings. These attributes can be part of the standard set of attributes provided by the target system or custom attributes that you add on the target system.

The following is the list of the "out-of-the-box" supported attributes for Oracle Identity Manager (the attribute names are from the User Form Label name):

- User Id
- Password
- Owner
- User Class
- Password Expire
- Group Profile
- Initial Menu
- Job Description
- Limit Capabilities
- Description Text
- Initial Program

Table 1–2 describes the complete set of supported attributes, including the previously listed "out-of-the-box" attributes. To add these attributes and make them available, see the following sections:

- Section 4.1.1, "Adding Target System Attributes for Provisioning"
- Section 4.1.2, "Adding Target System Attributes for Target Reconciliation"
- Section 4.1.3, "Adding Target System Attributes for Trusted Reconciliation"

Some attributes as indicated in the table are stored in an OS/400 Directory Entry object. See Appendix A, "Policies for OS/400 Accounts Migration."

Table 1–2 User Attributes for Target Resource Reconciliation and Provisioning

OIM Process Form Attribute Name	AS400 Connector Attribute Name	Native OS/400 Attribute	Description
Status	__ENABLE__	None	Boolean. Indicates whether the account is enabled and logins are allowed.
__LAST_LOGIN_DATE__	__LAST_LOGIN_DATE__	None	Long. Read-only. Last login date.
__LAST_PASSWORD_CHANGE_DATE__	__LAST_PASSWORD_CHANGE_DATE__	None	Long. Read-only. Date and time the password was last updated.
Account Name	__NAME__	User profile name	Required. Not updatable. OS/400 user profile name. The user profile name can be a maximum of 10 characters, including any letter (A-Z), a number (0-9), and the following special characters: pound (#), dollar ($), underscore (_), and at (@). The first character cannot be a number.
Password	__PASSWORD__	User password	Required. Guarded string. OS/400 user password. Value is encrypted.
PASSWORD_CHANGE_INTERVAL	PASSWORD_CHANGE_INTERVAL	None	Integer. Number of days between the date when the password is changed and the date when the password expires. Values can be -1 - 366: -1 - The user's password does not expire (*NOMAX). 0 - The system value QPWDEXPITV is used to determine the user's password expiration interval (*SYSVAL). 1–366 days.
Password Expire	__PASSWORD_EXPIRED__	None	Boolean. Indicates whether the password has expired.
ACCOUNTING_CODE	ACCOUNTING_CODE	ACGCDE	Accounting code associated with the user. Values can be a character value (15 characters, padded with blanks if fewer that 15 characters), *SAME, or *BLANK.
ADDRESS1	ADDRESS1	Directory entry attribute	First line of the user's address.
ADDRESS2	ADDRESS2	Directory entry attribute	Second line of the user's address.
ASTLVL	ASTLVL	ASTLVL	Assistance level. Sets which interface to use.
ATNPGM	ATNPGM	ATNPGM	Attention-key-handling program for this user
BUILDING	BUILDING	Directory entry attribute	Building name or number.
CCSID	CCSID	CCSID	Coded character set identifier.
CNTRYID	CNTRYID	CNTRYID	Country or region identifier.
COMPANY	COMPANY	Directory entry attribute	Company name.
CURLIB	CURLIB	CURLIB	Current library for jobs initiated by this user profile.
DAYS_UNTIL_PASSWORD_EXPIRES	DAYS_UNTIL_PASSWORD_EXPIRES	None	Integer. Read-only. Number of days until the password expires.
DEPARTMENT	DEPARTMENT	Directory entry attribute	Department name or code.
DLVRY	DLVRY	DLVRY	Delivery mode that specifies how messages sent to the message queue for this user are to be delivered.
FAX	FAX	Directory entry attribute	Fax telephone number.

Table 1–2 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Process Form Attribute Name	AS400 Connector Attribute Name	Native OS/400 Attribute	Description
First Name	FIRST_NAME	Directory entry attribute	User's first name. A maximum of 20 characters is allowed.
FULL_NAME	FULL_NAME	Directory entry attribute	User's full name.
GID	GID	GID	Long. Group identification number for this user profile. You can assign the GID to a user who does not have an associated group profile.
GROUP_AUTHORITY	GROUP_AUTHORITY	GRPAUT	Authority given to the group profile for newly created objects. Values can be *SAME, *NONE, *ALL, *CHANGE, *USE, or *EXCLUDE.
Group Profile	GROUP_PROFILE_NAME	GRPPRF	User's group profile name whose authority is used if no specific authority is given for the user or *NONE.
HIGHEST_SCHEDULING_PRIORITY	HIGHEST_SCHEDULING_PRIORITY	PTYLMT	Integer. highest scheduling priority the user is allowed to have for each job submitted to the system. Values can be 0 (highest) through 9 (lowest).
HOMEDIR	HOMEDIR	HOMEDIR	Pathname of the user's home directory.
Initial Menu	INLMNU	INLMNU	Initial menu displayed when the user signs on the system if the user's routing program is the command processor.
Initial Program	INLPGM	INLPGM	Initial program to call when a user signs on. An initial program runs before the initial menu, if any, is displayed.
Job Description	JOBD	JOBD	Fully qualified integrated file-system path name of the job description used for jobs that start through subsystem work station entries.
JOB_TITLE	JOB_TITLE	Directory entry attribute	Job title for this user.
KBDBUF	KBDBUF	KBDBUF	Keyboard buffering used when a job is initiated for this user.
LANGID	LANGID	LANGID	Language identifier for the user.
Last Name	LAST_NAME	Directory entry attribute	User's last name. A maximum of 40 characters is allowed.
Limit Capabilities	LMTCPB	LMTCPB	Limit capabilities for this user.
LMTDEVSSN	LMTDEVSSN	LMTDEVSSN	Limit for number of device sessions for this user.
LOCATION	LOCATION	Directory entry attribute	Location for this user.
MAXSTG	MAXSTG	MAXSTG	Maximum amount of auxiliary storage (in kilobytes) assigned to store permanent objects owned by this user profile. Values can be: -1 – As much storage as is required is assigned to this profile (*NOMAX). Maximum amount of storage for the user, in kilobytes (1 kilobyte equals 1024 bytes).
MIDDLE_NAME	MIDDLE_NAME	Directory entry attribute	User's middle name.
MSGQ	MSGQ	MSGQ	Message queue where messages are sent for this user.
OFFICE	OFFICE	Directory entry attribute	Office name or number.
OUTQ	OUTQ	OUTQ	Output queue for this user profile.
Owner	OWNER	OWNER	Owner of new objects created by this user.

Table 1–2 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Process Form Attribute Name	AS400 Connector Attribute Name	Native OS/400 Attribute	Description
PREFERRED_NAME	PREFERRED_NAME	Directory entry attribute	User's preferred name.
PRTDEV	PRTDEV	PRTDEV	Default print device for this user.
SIGN_ON_ATTEMPTS_NOT_VALID	SIGN_ON_ATTEMPTS_NOT_VALID	None	Integer. Read-only. Number of invalid login attempts since the last successful login.
Special Authority	SPCAUT	SPCAUT	List of special authorities for this user. Can have multiple values.
SPCENV	SPCENV	SPCENV	Special environment for this user.
SRTSEQ	SRTSEQ	SRTSEQ	Sort sequence table used for string comparisons for this user.
STORAGE_USED	STORAGE_USED	None	Integer. Read-only. Amount of auxiliary storage in kilobytes occupied by this user's owned objects. Default is 12 kilobytes.
Supplemental Group	SUPGRPPRF	SUPGRPPRF	List of the user's supplemental group profiles. Can have multiple values. To update the Supplemental Group attribute, the Group Profile attribute must have a non-empty value. That is, to populate supplemental groups, a primary group (Group Profile) must already be defined.
TELEPHONE	TELEPHONE	Directory entry attribute	Use's telephone number.
Description Text	TEXT	TEXT	Text up to 40 characters describing the object (OS/400 account).
UID	UID	UID	Long. User identification number. Range is 1 to 4294967294. The UID must not already be assigned to another user profile. **Note**. The UID is read-only (that is, non-creatable and non-updatable).
User Class	USRCLS	USRCLS	Type of user associated with this user profile: security officer, security administrator, programmer, system operator, or user.
USROPT	USROPT	USROPT	Level of help information detail to be shown and the function of the Page Up and Page Down keys by default.

1.5.2 Process Form Fields Used for Target Provisioning and Reconciliation

The following table describes the process form fields that the AS400 connector uses for target provisioning and reconciliation.

Table 1–3 Process Form Fields Used for Target Provisioning and Reconciliation

Process Form Field Label	Field Type	Description
Account Name	TextField	OS/400 user profile name. The user profile name can be a maximum of 10 characters, including any letter (A-Z), a number (0-9), and the following special characters: pound (#), dollar ($), underscore (_), and at (@). The first character cannot be a number.
Description Text	TextField	Text up to 40 characters describing the object (OS/400 account).
First Name	TextField	User's first name. A maximum of 20 characters is allowed.
Group Profile	LookupField	User's group profile name whose authority is used if no specific authority is given for the user or *NONE.
Initial Menu	TextField	Initial menu displayed when the user signs on the system if the user's routing program is the command processor.
Initial Program	TextField	Initial program to call when a user signs on. An initial program runs before the initial menu, if any, is displayed.
Job Description	TextField	Fully qualified integrated file-system path name of the job description used for jobs that start through subsystem work station entries.
Last Name	TextField	User's last name. A maximum of 40 characters is allowed.
Limit Capabilities	TextField	Limit capabilities for this user.
Owner	TextField	Owner of new objects created by this user.
Password	PasswordField	OS/400 user password. Value is encrypted.
Password Expire	CheckBox	Boolean. Indicates whether the password has expired.
Server	ITResourceLookupField	Name of the IT Resource instance.
Special Authority	TextField	List of special authorities for this user. Can have multiple values.
Supplemental Group	TextField	List of the user's supplemental group profiles. Can have multiple values.
User Class	TextField	Type of user associated with this user profile: security officer, security administrator, programmer, system operator, or user.
User Id	TextField	OS/400 user profile name.

The following table describes the AS400 connector mapping of form fields to user attributes for target resource provisioning and reconciliation.

Table 1–4 Mapping Form Fields to User Attributes for Target Resource Provisioning and Reconciliation

Process Form Field Label	OS/400 Attribute
Account Name	__NAME__
Description Text	TEXT

Table 1–4 (Cont.) Mapping Form Fields to User Attributes for Target Resource Provisioning and Reconciliation

Process Form Field Label	OS/400 Attribute
First Name	FIRST_NAME
Group Profile	GROUP_PROFILE_NAME
Initial Menu	INLMNU
Initial Program	INLPGM
Job Description	JOBD
Last Name	LAST_NAME
Limit Capabilities	LMTCPB
Owner	OWNER
Password	__PASSWORD__
Password Expire	__PASSWORD_EXPIRED__
Special Authority	SPCAUT
Status	__ENABLE__
Supplemental Group	SUPGRPPRF
User Class	USRCLS
User Id	__UID__

The following table describes the AS400 connector mapping of form fields to user attributes for trusted source reconciliation.

Table 1–5 Mapping Form Fields to User Attributes for Trusted Source Reconciliation

OIM User Form Field	OS/400 Attribute
First Name	FIRST_NAME
Last Name	LAST_NAME
Status	__ENABLE__
User Id	__UID__
User Login	__NAME__

1.5.3 Reconciliation

Reconciliation involves pulling identities from the target resource (OS/400) to the destination (Oracle Identity Manager). Reconciliation is based on following criteria:

- Destination type: trusted and target reconciliation
- Scope: full or incremental reconciliation

The scheduled task name includes the keywords trusted or target to determine the type of destination. By choosing the scheduled task, it is determined whether trusted or target reconciliation is launched.

This section describes the following subsections:

- Section 1.5.3.1, "Common Reconciliation Parameters"
- Section 1.5.3.2, "Full and Incremental Reconciliation Modes"

- Section 1.5.4.1, "Delete Reconciliation"
- Section 1.5.4.2, "Lookup Reconciliation"

Caution: Make sure that you use the right IT Resource type (trusted or target) with the respective scheduled task. The type of IT resource is determined by the value for the Configuration Lookup IT resource parameter:

- If Configuration Lookup is Lookup.AS400.Configuration, then it is target mode.
- If Configuration Lookup is Lookup.AS400.Configuration.Trusted, then it is trusted mode.

1.5.3.1 Common Reconciliation Parameters

Common reconciliation parameters for the AS400 connector are:

- Filter - optional filter to limit the number of reconciled accounts or to select specific set of users.
- IT Resource Name - required parameter specifying the name of IT Resource instance to recon.
- Object Type (constant) – User object class.
- Resource Object Name – constant parameter determining what OIM Resource Object to use for reconciliation.

1.5.3.2 Full and Incremental Reconciliation Modes

When the reconciliation scheduled task is launched for the first time, it is run in full reconciliation mode. Subsequent runs are automatically in incremental mode.

It is possible to switch manually between full and incremental modes by emptying the Latest Token field on the scheduled task.

The following scheduled tasks provide for optional incremental reconciliation: AS400Connector Target User Reconciliation and AS400Connector Trusted User Reconciliation.

Advanced Incremental Reconciliation

The format of Latest Token is altered by setting the Recon Date Format scheduled task parameter. The formatting string needs to follow the standard pattern used in Java. For information, see the Javadoc for java.text.SimpleDateFormat class:

http://download.oracle.com/javase/6/docs/api/java/text/SimpleDateFormat.html

By default, the Latest Token is a long value that specifies the Unix/POSIX time.

1.5.3.3 Delete Reconciliation

AS400 supports both trusted and target reconciliation of deleted accounts. Target reconciliation evaluate which OIM users have lost their account on OS/400 resource, and unassign this resource in OIM. Trusted delete recon goes further, and deletes the OIM User.

1.5.3.4 Group Lookup Reconciliation

Before the first use of provisioning with the AS400 connector, it is recommended that you launch Lookup Reconciliation. This Lookup Reconciliation populates the Lookup.AS400.Groups table with the groups available on the IT Resource that is being reconciled.

Lookup Reconciliation must be launched on the target mode IT Resource (that is, the value of the "Configuration Lookup" property on the IT Resource equals "Lookup.Configuration.AS400").

The reconciliation is performed by the AS400Connector Lookup Reconciliation scheduled task. The target IT Resource Name is used for the Lookup Reconciliation of the groups.

These parameters are constants:

- Code key attribute – connector attribute that will be used as key of lookup
- Decode key attribute – connector attribute specifying the value of lookup
- Object type – Group

For more information, see Section 3.1, "Scheduled Job for Lookup Field Synchronization."

1.5.4 Full or Incremental Reconciliation

In full reconciliation, all records are fetched from the target system to Oracle Identity Manager during the first reconciliation run performed on the target system. From the second reconciliation run onward, incremental reconciliation meaning accounts that have been added, modified, or deleted after the recorded timestamp are fetched for reconciliation.

The following scheduled jobs are used to automate full reconciliation:

- AS400Connector Target User Reconciliation
- AS400Connector Trusted User Reconciliation

1.5.4.1 Delete Reconciliation

The following scheduled jobs are used for delete reconciliation:

- AS400Connector Trusted User Delete Reconciliation
- AS400Connector Target User Delete Reconciliation

1.5.4.2 Lookup Reconciliation

In Lookup reconciliation, groups that exists on the target and can be assigned to the user are fetched from the target system to Oracle Identity Manager. The AS400Connector Lookup Reconciliation scheduled job is used to automate lookup reconciliation.

1.5.5 Support for Reconciliation of Account Status

During a reconciliation run, the connector can fetch status information along with the rest of the account data.

1.5.6 Features Provided by the Identity Connector Framework

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager and Oracle Waveset connectors require. The ICF also uses classpath isolation, which allows the AS400 connector to co-exist with legacy versions of the connector.

For more information, see Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

1.5.7 Support for Scheduled Tasks

Table 1–6 shows an overview of the AS400 connector scheduled task capabilities. For more information, see Section 3.3, "Configuring Scheduled Jobs."

Table 1–6 Overview of AS400 Connector Scheduled Task Capabilities

Scheduled Task	Capability
AS400Connector Target User Reconciliation	Trusted: Not available Target: Available Full: Empty "Latest Token" scheduled task parameter controls reconciliation. Incremental: Populated "Latest Token" scheduled task parameter controls incremental reconciliation. Delete: Not available
AS400Connector Trusted User Reconciliation	Trusted: Available Target: Not available Full: Empty "Latest Token" scheduled task parameter controls reconciliation. Incremental: Populated "Latest Token" scheduled task parameter controls incremental reconciliation. Delete: Not available
AS400Connector Target User Delete Reconciliation	Trusted: Not available Target: Available Full: Not available Incremental: Not available Delete: Available
AS400Connector Trusted User Delete Reconciliation	Trusted: Available Target: Not available Full: Not available Incremental: Not available Delete: Available

1.5.8 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target system. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps

reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource type. For example, if you have three IT resources for three installations of the target system, then three connection pools are created, one for each target system installation.

The AS400 connector uses Identity Connector Framework (ICF) connection pooling. For more information, see Section 4.3, "Configuring Connection Pooling."

1.5.9 Support for the Connector Server

If required by your deployment, you can deploy the AS400 connector in the Connector Server. For more information, see Section 2.1, "AS400 Connector Deployment Architecture With the Connector Server."

1.6 Lookup Definitions Used During Connector Operations

This section describes the following AS400 connector Lookup definitions:

- Section 1.6.1, "AS400 Connector Lookup Definitions Overview"
- Section 1.6.2, "Lookup.Configuration.AS400 Definition"
- Section 1.6.3, "Lookup.AS400.UM.Configuration Definition"
- Section 1.6.4, "Lookup.AS400.UM.ProvAttrMap Definition"
- Section 1.6.5, "Lookup.AS400.UM.ReconAttrMap Definition"
- Section 1.6.6, "Lookup.Configuration.AS400.Trusted Definition"
- Section 1.6.7, "Lookup.AS400.UM.ReconAttrMap.Trusted Definition"
- Section 1.6.8, "Lookup.AS400.UM.Configuration.Trusted Definition"
- Section 1.6.9, "Lookup.AS400.UM.TrustedDefaults Definition"
- Section 1.6.10, "Lookup.AS400.Groups Definition for Reconciliation for Groups"

1.6.1 AS400 Connector Lookup Definitions Overview

The AS400 connector Lookup definitions provide various information to the Oracle Identity Manager engine. These Lookup definitions are either prepopulated with values, or values must be manually entered in a definition after the connector is deployed:

- Configuration of the AS400 connector (for example, Lookup.Configuration.AS400): Top-level Lookup element that contains the connector version. The configuration references the following user management (UM) configuration Lookup.
- User management (UM) configuration (for example, Lookup.AS400.UM.Configuration): Hub that points to subordinate lookups that contain information about attribute mapping for reconciliation and provisioning.
- Provisioning attribute map (for example, Lookup.AS400.UM.ProvAttrMap): Mapping of OIM user attributes (key) to connector attributes (value) for provisioning.
- Reconciliation attribute map (for example, Lookup.AS400.UM.ReconAttrMap): Mapping of OIM user attributes (key) to connector attributes (value) for reconciliation.

- Holder of lookup reconciliation values (Lookup.AS400.Groups): Whenever group reconciliation is performed, this lookup is populated with group names.

1.6.2 Lookup.Configuration.AS400 Definition

The Lookup.Configuration.AS400 definition contains the entries shown in Table 1–7.

Table 1–7 Lookup.Configuration.AS400 Entries

Key Code	Decode	Description
Connector Name	org.identityconnectors.as400.AS400Connector	This entry holds the name of the connector class. Do not modify this entry.
Bundle Name	org.identityconnectors.as400	This entry holds the name of the connector bundle class. Do not modify this entry.
Bundle Version	1.0.0	This entry holds the version of the connector bundle class. Do not modify this entry.
User Configuration Lookup	Lookup.AS400.UM.Configuration	This entry holds the name of the lookup definition that stores configuration information used during user management operations. Do not modify this entry.

1.6.3 Lookup.AS400.UM.Configuration Definition

The Lookup.AS400.UM.Configuration definition contains the entries shown in Table 1–8.

Table 1–8 Lookup.AS400.UM.Configuration Entries

Key Code	Decode	Description
Provisioning Attribute Map	Lookup.AS400.UM.ProvAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during provisioning operations.
Recon Attribute Map	Lookup.AS400.UM.ReconAttrMap	This entry holds the name of the lookup definition that stores attribute mappings between Oracle Identity Manager and the target system. This lookup definition is used during reconciliation.
Unique Id Form Field	UD_AS400CON_UID	This entry holds the name of the process form field (column) that stores Unique ID values. If you create a copy of the process form, then enter the name of the field (column) in the new process form that stores Unique ID values.

1.6.4 Lookup.AS400.UM.ProvAttrMap Definition

The Lookup.AS400.UM.ProvAttrMap definition holds mappings between process form fields and target system attributes. These Lookup definitions are used during provisioning. These lookup definitions are preconfigured.

The Lookup.AS400.UM.ProvAttrMap definition contains the entries shown in Table 1–9.

Table 1–9 Lookup.AS400.UM.ProvAttrMap Entries

Key	Value
Last Name	LAST_NAME
UD_AS400CSP~Special Authority	SPCAUT
User Id	__UID__
User Class	USRCLS
Password	__PASSWORD__
Account Name	__NAME__
Initial Menu	INLMNU
Owner	OWNER
Job Description	JOBD
Password Expire	__PASSWORD_EXPIRED__
Description Text	TEXT
First Name	FIRST_NAME
Initial Program	INLPGM
UD_AS400CSG~Supplemental Group[Lookup]	SUPGRPPRF
Limit Capabilities	LMTCPB
Group Profile[Lookup]	GROUP_PROFILE_NAME

You can add entries in this Lookup definition if you want to map new target system attributes for provisioning. See Section 4.1.1, "Adding Target System Attributes for Provisioning."

1.6.5 Lookup.AS400.UM.ReconAttrMap Definition

The Lookup.AS400.UM.ReconAttrMap definition holds mappings between process form fields and target system attributes. These Lookup definitions are used during reconciliation. These Lookup definitions are preconfigured.

The Lookup.AS400.UM.ReconAttrMap definition contains the entries shown in Table 1–10.

Table 1–10 Lookup.AS400.UM.ReconAttrMap Entries

Key	Value
Status	__ENABLE__
Description Text	TEXT
Special Authorities~Special Authority	SPCAUT
Owner	OWNER
Account Name	__NAME__
User Id	__UID__
Initial Program	INLPGM
User Class	USRCLS
Job Description	JOBD

Table 1–10 (Cont.) Lookup.AS400.UM.ReconAttrMap Entries

Key	Value
Limit Capabilities	LMTCPB
Password Expire	__PASSWORD_EXPIRED__
Initial Menu	INLMNU
Supplemental Groups~Supplemental Group[Lookup]	SUPGRPPRF
Group Profile[Lookup]	GROUP_PROFILE_NAME
Last Name	LAST_NAME
First Name	FIRST_NAME

You can add entries in this Lookup definition if you want to map new target system attributes for reconciliation. See Section 4.1.2, "Adding Target System Attributes for Target Reconciliation" and Section 4.1.3, "Adding Target System Attributes for Trusted Reconciliation."

1.6.6 Lookup.Configuration.AS400.Trusted Definition

The Lookup.Configuration.AS400.Trusted definition contains the entries shown in Table 1–11.

Table 1–11 Lookup.Configuration.AS400.Trusted Entries

Key	Value
Bundle Name	org.identityconnectors.as400
Connector Name	org.identityconnectors.as400.AS400Connector
User Configuration Lookup	Lookup.AS400.UM.Configuration.Trusted
Bundle Version	1.0.0

1.6.7 Lookup.AS400.UM.ReconAttrMap.Trusted Definition

The Lookup.AS400.UM.ReconAttrMap.Trusted definition contains the entries shown in Table 1–12.

Table 1–12 Lookup.AS400.UM.ReconAttrMap.Trusted Entries

Key	Value
Status	__ENABLE__
Last Name	LAST_NAME
User Login	__NAME__
First Name	FIRST_NAME
User Id	__UID__

1.6.8 Lookup.AS400.UM.Configuration.Trusted Definition

The Lookup.AS400.UM.Configuration.Trusted definition contains the entries shown in Table 1–13.

Table 1–13 Lookup.AS400.UM.Configuration.Trusted Entries

Key	Value
Unique Id Form Field	UD_AS400CON_UID
Recon Attribute Defaults	Lookup.AS400.UM.TrustedDefaults
Recon Attribute Map	Lookup.AS400.UM.ReconAttrMap.Trusted

1.6.9 Lookup.AS400.UM.TrustedDefaults Definition

The Lookup.AS400.UM.TrustedDefaults definition contains the entries shown in Table 1–14.

Table 1–14 Lookup.AS400.UM.TrustedDefaults Entries

Key	Value
Organization	Xellerate Users
Employee Type	Full-Time
User Type	End-User

1.6.10 Lookup.AS400.Groups Definition for Reconciliation for Groups

The Lookup.AS400.Groups is populated with the groups from the OS/400 target resource when Lookup Reconciliation is performed.

During a provisioning operation, you use the Group lookup field on the process form to specify a group for the user for whom the provisioning operation is being performed. The Group lookup field is populated with values from the `Lookup.AS400.Groups` lookup definition, which is automatically created on Oracle Identity Manager when you deploy the connector. However, to get it populated, an initial reconciliation should be explicitly launched.

The Code Key column contains the following format: `<IT Resource key~groupName>`. The Decode column has the format: `<IT Resource key~groupName>`.

The source of group names is the connector `__NAME__` attribute of the Group objectClass.

When you perform lookup field synchronization, entries in the Group lookup field on the target system are fetched to Oracle Identity Manager and populated in the `Lookup.AS400.Groups` lookup definition.

1.7 Resource Objects Used for Provisioning and Reconciliation

The AS400 connector uses the following Resource Objects:

- AS400 User
- AS400 Trusted User

See Also:

- See Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about reconciliation.
- See Managing Provisioning Tasks in *Oracle Fusion Middleware Performing Self Service Tasks with the Oracle Identity Manager* for conceptual information about provisioning.

This section discusses the following topics:

- Section 1.7.1, "User Provisioning Functions"
- Section 1.7.2, "Reconciliation Rules"
- Section 1.7.3, "Reconciliation Action Rules"

1.7.1 User Provisioning Functions

Provisioning involves creating or modifying account data on the target system through Oracle Identity Manager.

Table 1–15 lists the supported user provisioning functions and the adapters that perform these functions. The functions listed in the table correspond to either a single or multiple process tasks.

See Also: See Types of Adapters in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about process tasks adapters

Table 1–15 User Provisioning Functions

Function	Adapter
Create user	CREATEUSER
Update user	UPDATEATTRIBUTEVALUE For multivalued attributes: UPDATECHILDTABLEVALUES
Delete user	DELETEUSER
Enable or disable user	ENABLEUSER, DISABLEUSER
Change or reset password	UPDATEATTRIBUTEVALUE
Add or remove user from group	UPDATEATTRIBUTEVALUE

1.7.2 Reconciliation Rules

See Also: See the following sections in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about reconciliation matching and action rules:

- Creating Reconciliation Metadata (Developing Identity Connectors Using Java)
- Creating Reconciliation Metadata (Developing Identity Connectors Using .NET)

The following sections provide information about the reconciliation rules for this connector.

There are different reconciliation rules used for trusted and target reconciliation:

- AS400 Trusted User Recon Rule: User Login equals UserId, Resource Object: AS400 Trusted User
- AS400 User Recon Rule: User Login equals UserId, Resource Object: AS400 User

1.7.2.1 Viewing Reconciliation Rules in the Design Console

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for and open**AS400 User Recon Rule** or **AS400 Trusted User Recon Rule**.

1.7.3 Reconciliation Action Rules

Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See the following sections in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about setting or modifying a reconciliation action rule:

- Setting a Reconciliation Action Rule (Developing Identity Connectors using Java)
- Setting a Reconciliation Action Rule (Developing Identity Connectors using .NET)

The following sections provide information about the reconciliation rules for this connector:

- Section 1.7.3.1, "Reconciliation Action Rules for Reconciliation"
- Section 1.7.3.2, "Viewing Reconciliation Action Rules in the Design Console"

You can configure the Reconciliation Action Rules in the Design Console under the Resource Object tab, Object Reconciliation tab, and then Reconciliation Action Rules.

1.7.3.1 Reconciliation Action Rules for Reconciliation

Table 1–16 lists the action rules for reconciliation.

Table 1–16 Action Rules for Reconciliation

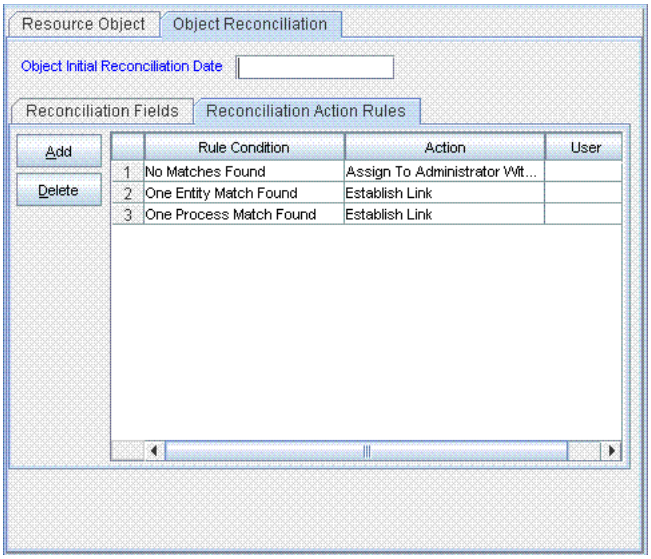
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

1.7.3.2 Viewing Reconciliation Action Rules in the Design Console

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**, and double-click **Resource Objects**.
3. If you want to view the **AS400 User Recon** rule for reconciliation, then search for and open the **AS400 User** resource object.
4. 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. Figure 1–2 shows the reconciliation action rules for reconciliation.

Figure 1–2 Reconciliation Action Rules



1.8 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes the procedures to perform if you want to extend the functionality of the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.
- Appendix A, "Policies for OS/400 Accounts Migration" describes the policies OS/400 account migration.

2

Deploying the Connector

This chapter contains the following sections:

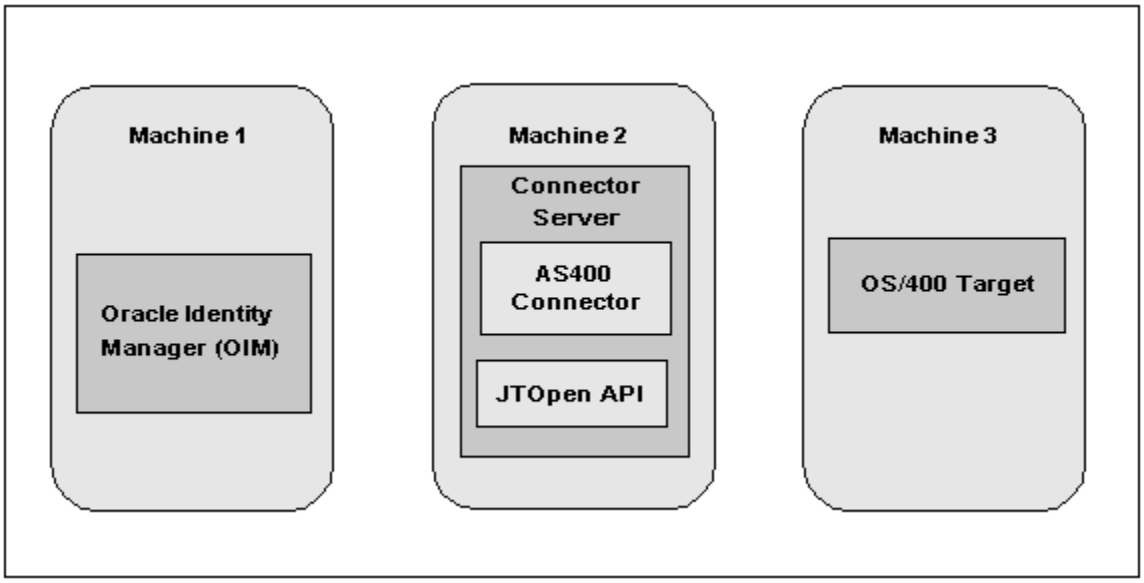
2.1 AS400 Connector Deployment Architecture With the Connector Server

You can deploy the AS400 connector either locally in Oracle Identity Manager or remotely in the Connector Server.

Note: In a production environment, it is recommended that you deploy the AS400 connector in the Connector Server.

The following figure shows the AS400 connector deployment architecture with the Connector Server.

Figure 2–1 Connector Deployment Architecture With the Connector Server



- Machine 1 has Oracle Identity Manager deployed.
- Machine 2 has the AS400 connector installed in the Connector Server. The Connector Server is part of the Identity Connector Framework (ICF).

  The jt400.jar file from the JTOpen library must be installed in the *CONNECTOR_SERVER_HOME*/lib directory.

  For detailed installation information, see Installing the Section 2.3.2, "Deploying the Connector Bundle in a Connector Server".
- Machine 3 has the OS/400 target deployed.

2.2 Preinstallation

Preinstallation information is divided across the following sections:

- Section 2.2.1, "Preinstallation on Oracle Identity Manager"
- Section 2.2.2, "Preinstallation on the Target System"
- Section 2.2.3, "Installing and Configuring the Connector Server"

2.2.1 Preinstallation on Oracle Identity Manager

This section describes the following topics for Oracle Identity Manager:

- Section 2.2.1.1, "Files and Directories on the Installation Media"
- Section 2.2.1.2, "Downloading and Installing the JTOpen Library"

2.2.1.1 Files and Directories on the Installation Media

The Oracle Identity Manager AS400 connector is distributed as a ZIP file named as400-11.1.1.6.0.zip. Table 2–1 describes the contents of this ZIP file.

Table 2–1 Files and Directories On the Installation Media

Directory	Description
bundle	org.identityconnectors.as400-1.0.0.jar
configuration	AS400-ConnectorInstaller.xml contains configuration information that is used during the connector installation.
datasets	■ ModifyProvisionedResource_AS400User.xml ■ ProvisionResource_AS400User.xml The format of these datasets is Oracle Metadata Service (MDS) XML. **Note:** Use these files only if you are using Oracle Identity Manager release prior to 11.1.2.
resources	AS400 connector properties files, including files containing localized versions of the text strings that are displayed in the Administrative and User Console. These text strings include GUI element labels and messages. as400.properties as400_ar.properties as400_da.properties as400_de.properties as400_es.properties as400_fr.properties as400_it.properties as400_ja.properties as400_ko.properties as400_pt_BR.properties as400_zh_CN.properties as400_zh_TW.properties as400_en_US.properties
xml	■ AS400-ConnectorConfig.xml contains information used to initialize the OIM data repository with connector integration artifacts. ■ AS400-Datasets.xml contains datasets for provisioning and modifying of the "AS400 User" Resource Object. The format of these datasets is Deployment Manager XML. **Note:** Use this file only if you are using Oracle Identity Manager release prior to 11.1.2.

2.2.1.2 Downloading and Installing the JTOpen Library

The AS400 connector requires the JTOpen library, which is not included in the connector bundle. You must download this library separately and include the jt400.jar file for the AS400 connector as follows:

1. Download the JTOpen library from the following location:
   http://jt400.sourceforge.net
2. Create a directory named as400-11.1.1.6.0 for the AS400 connector under the following directory:

   OIM_HOME/ConnectorDefaultDirectory/targetsystems-lib/

   The files in this directory are not shared with any other connectors, which helps to avoid version conflicts among shared libraries.
3. Copy the jt400.jar file to the directory you created in the previous step.

Note: If you are deploying the AS400 connector in the Connector Server, see Section 2.3.2, "Deploying the Connector Bundle in a Connector Server" for information about copying this file.

2.2.2 Preinstallation on the Target System

Preinstallation on the target system involves performing the following procedures:

- Section 2.2.2.1, "Creating a Target System User Account for AS400 Connector Operations"
- Section 2.2.1.2, "Downloading and Installing the JTOpen Library"

2.2.2.1 Creating a Target System User Account for AS400 Connector Operations

Note: The AS400 connector uses an account with the administrative privileges described below. For increased security, it is recommended that you create a separate account, apart from QSECOFR (the OS/400 security officer account).

The following administrative privileges are required for the AS400 connector:

- Create Account - CRT: To add an OS/400 user, the administrator must have the following privileges:
  - *SECADM special authority
  - *USE authority to the initial program, initial menu, job description, message queue, output queue, and attention-key-handling program if specified
  - *CHANGE and object management authorities to the group profile and supplemental group profiles, if specified
- Update Account - CHG: The administrator must have *SECADM special authority, and *OBJMGT and *USE authorities to the user profile being changed, to specify this command. *USE authority to the current library, program, menu, job description, message queue, print device, output queue, or ATTN key handling program is required to specify these parameters.
- Delete Account - DLT: The administrator must have use (*USE) and object existence (*OBJEXIST) authority to the user profile. The user must have existence, use, and delete authorities to delete a message queue associated with and owned by the user profile. The user profile cannot be deleted if a user is currently running under the profile, or if it owns any objects and OWNOBJOPT(*NODLT) is specified.

  All objects in the user profile must first either be transferred to new owners by using the Change Object Owner (CHGOBJOWN) command or be deleted from the system. This can also be accomplished by specifying OWNOBJOPT(*DLT) to delete the objects or OWNOBJOPT(*CHGOWN user-profile-name) to change the ownership.

  Authority granted to the user does not have to be specifically revoked by the Revoke Object Authority (RVKOBJAUT) command; it is automatically revoked when the user profile is deleted.

- Search or Reconcile Account - DSP: The administrator name can be specified as USRPRF(*ALL) or USRPRF(generic*-user-name) only when TYPE(*BASIC) and OUTPUT(*OUTFILE) are specified.

Note: If the administrator requires additional rights, use the following commands from the OS/400 console:

```
CRTUSRPRF USRPRF (adminUserName) AUT
(list-of-necessary-permissions)
CHGUSRPRF USRPRF (adminUserName) SPCAUT
(list-of-necessary-permissions)
```

The *list-of-necessary-permissions* can differ for each administrator and should be determined based on your deployment requirements.

Also, *USE and *CHANGE are values for the GRPAUT (Group Authority) parameter of the CHGUSRPRF command. Group Authority specifies the authority given to the group profile for newly created objects.

2.2.3 Installing and Configuring the Connector Server

To install and configure the Connector Server, follow these steps:

1. Create a new directory on the machine where you want to install the Connector Server. In this section, *CONNECTOR_SERVER_HOME* represents this directory.
2. Unzip the Connector Server package in your new directory from Step 1. The Connector Server package is available with the Identity Connector Framework (ICF).
3. In the ConnectorServer.properties file, set the following properties, as required by your deployment. The ConnectorServer.properties file is located in the conf directory.

Property	Description
connectorserver.port	Port on which the Connector Server listens for requests. The default is `8759`.
connectorserver.bundleDir	Directory where the connector bundles are deployed. The default is bundles.
connectorserver.libDir	Directory in which to place dependent libraries. The default is lib.

connectorserver.usessl	If set to true, the Connector Server uses SSL for secure communication. The default is `false`. If you specify `true`, use the following options on the command line when you start the Connector Server:
	`-Djavax.net.ssl.keyStore`
	`-Djavax.net.ssl.keyStoreType` (optional)
	`-Djavax.net.ssl.keyStorePassword`

connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the machine.
connectorserver.key	Connector Server key. The default password for this property is `changeit`.

4. Set the properties in the ConnectorServer.properties file, as follows:
   - To set connectorserver.key, run the Connector Server with the `/setKey` option.

     For more information, see Section 2.2.4.1, "Running the Connector Server on UNIX and Linux Systems" or Section 2.2.4.2, "Running the Connector Server on Windows Systems".
   - For all other properties, edit the ConnectorServer.properties file manually.
5. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

2.2.4 Running the Connector Server

This section describes how to run the Connector Server, depending on your platform:

- Section 2.2.4.1, "Running the Connector Server on UNIX and Linux Systems"
- Section 2.2.4.2, "Running the Connector Server on Windows Systems"

2.2.4.1 Running the Connector Server on UNIX and Linux Systems

To run the Connector Server on UNIX and Linux systems, use the connectorserver.sh script, as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Section 2.2.3, "Installing and Configuring the Connector Server".
2. Change to the *CONNECTOR_SERVER_HOME*/bin directory.
3. Use the `chmod` command to set the permissions to make the connectorserver.sh script executable.
4. Run the connectorserver.sh script. The script supports the following options.

Option	Description
/run [-J*java-option*]	Runs the Connector Server in the console. Optionally, you can specify one or more Java options. For example, to run the Connector Server with SSL: `./connectorserver.sh /run -J-Djavax.net.ssl.keyStore=mykeystore.jks -J-Djavax.net.ssl.keyStorePassword=password`
/start [-J*java-option*]	Runs the Connector Server in the background. Optionally, you can specify one or more Java options.
/stop	Stops the Connector Server, waiting up to 5 seconds for the process to end.
/stop *n*	Stops the Connector Server, waiting up to *n* seconds for the process to end.
/stop -force	Stops the Connector Server. Waits up to 5 seconds and then uses the kill -KILL command, if the process is still running.
/stop *n* -force	Stops the Connector Server. Waits up to *n* seconds and then uses the kill -KILL command, if the process is still running.
/setKey *key*	Sets the Connector Server key. The connectorserver.sh script stores the hashed value of *key* in the connectorserver.key property in the ConnectorServer.properties file.

2.2.4.2 Running the Connector Server on Windows Systems

To run the Connector Server on Windows systems, use the ConnectorServer.bat script as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Section 2.2.3, "Installing and Configuring the Connector Server".
2. Change to the *CONNECTOR_SERVER_HOME*\bin directory and run the ConnectorServer.bat script.

   The ConnectorServer.bat script supports the following options:

Option	Description
/install [*serviceName*] ["-J *java-option*"]	Installs the Connector Server as a Windows service. Optionally, you can specify a service name and Java options. If you do not specify a service name, the default name is ConnectorServerJava.
/run ["-J *java-option*"]	Runs the Connector Server from the console. Optionally, you can specify Java options. For example, to run the Connector Server with SSL: `ConnectorServer.bat /run "-J-Djavax.net.ssl.keyStore=mykeystore.jks" "-J-Djavax.net.ssl.keyStorePassword=password"`
/setKey [*key*]	Sets the Connector Server key. The ConnectorServer.bat script stores the hashed value of the key in the connectorserver.key property in the ConnectorServer.properties file.
/uninstall [*serviceName*]	Uninstalls the Connector Server. If you do not specify a service name, the script uninstalls the ConnectorServerJava service.

3. To stop the Connector Server, stop the respective Windows service.

2.3 Installation

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

- To run the connector code locally in Oracle Identity Manager, perform the procedure described in Section 2.3.1, "Installing the AS400 Connector in Oracle Identity Manager."
- To run the connector code remotely in a Connector Server, perform the procedures described in Section 2.3.1, "Installing the AS400 Connector in Oracle Identity Manager" and Section 2.3.2, "Deploying the Connector Bundle in a Connector Server."

2.3.1 Installing the AS400 Connector in Oracle Identity Manager

In this scenario, you install the connector in Oracle Identity Manager using the Connector Installer.

Note:

In this guide, the term **Connector Installer** is used to refer to the Install Connectors feature of Oracle Identity System Administration and Oracle Identity Self Service.

To run the Connector Installer:

1. Download the connector package (ZIP file) from the Oracle Technology Network site.
2. Unzip the connector package and copy the contents into one of the *OIM_HOME*/server/ConnectorDefaultDirectory directory.

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

3. If you have not already done so, create a directory in *OIM_HOME*/ConnectorDefaultDirectory/targetsystems-lib with the same name as the connector package. For the AS400 connector, this name is as400-11.1.1.6.0. For example:

   OIM_HOME/ConnectorDefaultDirectory/targetsystems-lib/as400-11.1.1.6.0

   Copy the jt400.jar file from the JTOpen library to this directory.

   For more information, see Section 2.2.1.2, "Downloading and Installing the JTOpen Library."
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector.**
   - For Oracle Identity Manager release 11.1.2.*x* or later:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click **Manage Connector.**
5. In the Manage Connector page, click **Install.**
6. From the Connector List select AS400 11.1.1.6.0. This list displays the names and release numbers of connectors whose installation files you can copy into the default connector installation directory:

   OIM_HOME/server/ConnectorDefaultDirectory

   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 AS400 11.1.1.6.0.
7. Click **Load**.

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

   The following tasks are performed in sequence:

   a. Configuration of connector libraries

   b. Import of the connector XML files (by using the Deployment Manager)

   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. If a task fails, then make the required correction and perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 3.

9. 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 PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.4.6, "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 tasks that are created when you installed the connector.

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

   Note: 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.

2.3.2 Deploying the Connector Bundle in a Connector Server

To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in Section 2.3.1, "Installing the AS400 Connector in Oracle Identity Manager."

Note:

- You can download the Connector Server from the Oracle Technology Network web page.
- See Section 2.4.10, "Creating the IT Resource for the Connector Server" for related information.
- See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for more information about installing, configuring, and running the Connector Server.

To install the AS400 connector into the Connector Server, follow these steps:

1. Stop the Connector Server.

Note: You can download the necessary Java Connector Server from the Oracle Technology Network web page.

2. Copy the AS400 connector bundle into the CONNECTOR_SERVER_HOME/bundles directory.
3. Copy the jt400.jar file to the CONNECTOR_SERVER_HOME/lib directory.
4. Start the Connector Server.
5. After the Connector Server is running, create a Connector Server IT Resource in Oracle Identity Manager.
6. Set the "Connector Server Name" parameter on the AS400 Resource to the IT Resource name you created in the previous step.

For information about starting and stopping the Connector Server, see Section 2.2.4.1, "Running the Connector Server on UNIX and Linux Systems" or Section 2.2.4.2, "Running the Connector Server on Windows Systems".

2.4 Postinstallation

Postinstallation steps are divided across the following sections:

- Section 2.4.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
- Section 2.4.2, "Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later"
- Section 2.4.3, "Configuring Password Changes for Newly Created Accounts"
- Section 2.4.4, "Enabling Request-Based Provisioning"
- Section 2.4.5, "Changing to the Required Input Locale"
- Section 2.4.6, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.4.7, "Enabling Logging"
- Section 2.4.8, "Configuring the IT Resource"
- Section 2.4.9, "Configuring SSL for the Connector"
- Section 2.4.10, "Creating the IT Resource for the Connector Server"

- Section 2.4.11, "Localizing Field Labels in UI Forms"

2.4.1 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- Section 2.4.1.1, "Creating and Activating a Sandbox"
- Section 2.4.1.2, "Creating a New UI Form"
- Section 2.4.1.3, "Creating an Application Instance"
- Section 2.4.1.4, "Publishing a Sandbox"
- Section 2.4.1.5, "Harvesting Entitlements and Sync Catalog"
- Section 2.4.1.6, "Updating an Existing Application Instance with a New Form"

2.4.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes.** The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox.** The Create Sandbox dialog box is displayed.
3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
5. Click **Save and Close.** A message is displayed with the sandbox name and creation label.
6. Click **OK.** The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. Select the sandbox that you created.
8. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
9. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

2.4.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see Managing Forms in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer.**
2. Under Search Results, click **Create.**
3. Select the resource type for which you want to create the form.
4. Enter a form name and click **Create.**

2.4.1.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see Managing Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances.**
2. Under Search Results, click **Create.**
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**
4. In the Form drop-down list, select the newly created form and click **Apply.**
5. Publish the application instance for a particular organization.

2.4.1.4 Publishing a Sandbox

To publish the sandbox that you created in Section 2.4.1.1, "Creating and Activating a Sandbox":

1. Close all the open tabs and pages.
2. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Section 2.4.1.1, "Creating and Activating a Sandbox."
3. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
4. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.4.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Section 3.1, "Scheduled Job for Lookup Field Synchronization."
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.4.1.6 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Section 2.4.1.1, "Creating and Activating a Sandbox."
2. Create a new UI form for the resource as described in Section 2.4.1.2, "Creating a New UI Form."
3. Open the existing application instance.

4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in Section 2.4.1.4, "Publishing a Sandbox."

2.4.2 Enabling the Reset Password Option in Oracle Identity Manager 11.1.2.1.0 or Later

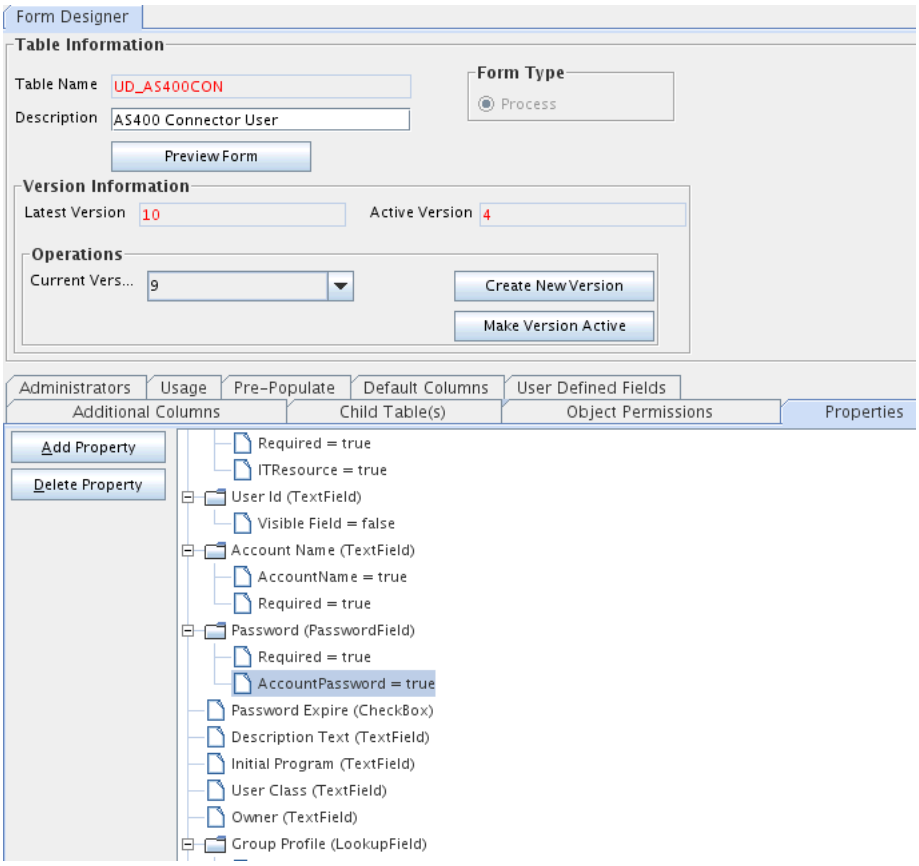
In Oracle Identity Manager release 11.1.2.1.0 or later, you can reset password for an account after logging in as the user by navigating to My Access, Accounts tab.

The Reset Password option is enabled for only those accounts that follow the UD_*FORMNAME*_PASSWORD naming convention for the password field. Otherwise, this option would be disabled as shown in the following sample screenshot:

To enable the Reset Password option in Oracle Identity Manager release 11.1.2.1.0 or later:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **Form Designer.**
3. Enter `UD_AS400` in the Table Name field and click the **Query for records** button.
4. Click **Create New Version.**
5. In the Create a New Version dialog box, specify the version name in the Label field, save the changes, and then close the dialog box.
6. From the **Current Version** list, select the newly created version.
7. Click the **Properties** tab.
8. Select the password field, and click **Add Property.**
9. From the Property Name list, select **AccountPassword.**
10. In the Property Value field, enter `true`.
11. Click **Save.**

    The password field is tagged with the `AccountPassword = true` property as shown in the following screenshot:



12. Click **Make Version Active.**

13. Update the application instance with the new form as described in Section 2.4.1.6, "Updating an Existing Application Instance with a New Form."

2.4.3 Configuring Password Changes for Newly Created Accounts

By default, when a user is created, a password should also be specified.

To configure the AS400 connector so that a newly created user is prompted for a password change at the first logon, check the "Password Expire" checkbox during the provisioning process.

The user will then be prompted to specify a new password on the next logon.

2.4.4 Enabling Request-Based Provisioning

In request-based provisioning, an end user creates a request for a resource or entitlement by using the Administrative and User Console. Administrators or other users cannot create requests for a particular user. Requests can be viewed and approved by approvers designated in Oracle Identity Manager.

Note: Perform this procedure only if you are using Oracle Identity Manager release prior to 11.1.2. The direct provisioning feature of the connector is automatically disabled when you enable request-based provisioning. Therefore, do not enable request-based provisioning if you want to use the direct provisioning.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.
- Direct provisioning cannot be used if you enable request-based provisioning.

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

- Section 2.4.4.1, "Copying Predefined Request Datasets"
- Section 2.4.4.2, "Importing Request Datasets into MDS"
- Section 2.4.4.3, "Enabling the Auto Save Form Feature"
- Section 2.4.4.4, "Running the PurgeCache Utility"

2.4.4.1 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 is the list of predefined request datasets available in the datasets directory on the installation media. The filenames are:

- ModifyProvisionedResource_AS400User.xml
- ProvisionResource_AS400User.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\AS400

> **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.

2.4.4.2 Importing Request Datasets into MDS

All request datasets (predefined or generated) must be imported into 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. Set up the environment for running the MDS Import utility as follows:

a. Set Environment Variable: Set the `OIM_ORACLE_HOME` environment variable to the Oracle Identity Management Oracle home directory inside the Middleware home directory. For example, for Microsoft Windows, set the `OIM_ORACLE_HOME` environment variable to C:\Oracle\Middleware\Oracle_IDM1\ directory.

b. Set Up the Properties File: Set the necessary properties in the `weblogic.properties` file, which is located in the same folder as the 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 2.4.4.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\Exchng directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

Table 2–2 Parameters in the Properties File

Property Name	Description	Notes
wls_servername	Name of the Oracle WebLogic Server on which Oracle Identity Manager is deployed	
application_name	The application name	Value is: ▪ `oim` if importing/exporting an out-of-the-box event handler. ▪ `OIMMetadata` for customizable metadata. If importing or exporting custom data, set application_name to OIMMetadata.
metadata_from_loc	Directory location from which an XML file should be imported. This property is used by weblogicImportMetadata.sh script.	Microsoft Windows paths include // as file or directory separator.
metadata_to_loc	Directory location from which an XML file should be imported. This property is used by weblogicExportMetadata.sh script.	Microsoft Windows paths include // as file or directory separator.
metadata_files	Full path and name of an XML file. This property is used by weblogicExportMetadata.sh and weblogicDeleteMetadata.sh scripts.	For example, you may specify /file/User.xml to export a user entity definition. You can indicate multiple xml files as comma-separated values.

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 values for the following:

   - `Please enter your username [weblogic]`

     Enter the username used to log in to the Oracle WebLogic Server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to the Oracle 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*

2.4.4.3 Enabling the Auto Save Form Feature

The Auto Save Form feature designates whether Oracle Identity Manager suppresses the display of the custom form associated with the provisioning process or displays it and allows a user to supply it with data each time the process is instantiated.

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 **AS400 User Process Form** process definition.
4. Select the **Auto Save Form** check box.

   Selecting this check box causes the data in the custom process form to be automatically saved without displaying the form. If you select this check box, you must supply either system-defined data or ensure that an adapter is configured to populate the form with the required data because the user will not be able to access the form.
5. Click **Save**.

2.4.4.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.4.6, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.4.5 Changing to the Required Input Locale

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

You may require the assistance of the system administrator to change to the required input locale.

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. 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, 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:

   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
   ```

   - 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.

2.4.7 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. Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. 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:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

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

- FINE, FINER, FINEST

  These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These message types are mapped to ODL message type and level combinations as shown in Table 2–3.

Table 2–3 Log Levels and ODL Message Type: Level Combinations

Java Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SEVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

```
<log_handler name='OIMCP.AS400' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="ORG.IDENTITYCONNECTORS.AS400" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="OIMCP.AS400"/>
     <handler name="console-handler"/>
   </logger>
```

   b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–3 lists the supported message type and level combinations.

   Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

   The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]**:

```
<log_handler name='OIMCP.AS400' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="ORG.IDENTITYCONNECTORS.AS400" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="OIMCP.AS400"/>
     <handler name="console-handler"/>
   </logger>
```

   With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:

   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:

   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```

   Replace ***FILENAME*** with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.4.8 Configuring the IT Resource

Configuring the IT resource includes these tasks:

- Section 2.4.8.1, "Creating a New IT Resource"
- Section 2.4.8.2, "Specifying Values for the IT Resource Parameters"

> **Note:** If you have configured your target system as a trusted source, then create an IT resource of type **AS400.** For example, AS400 Trusted. The parameters of this IT resource are the same as the parameters of the IT resources described in Table 2–4 of this section. See Creating IT Resources in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about creating an IT resource.

2.4.8.1 Creating a New IT Resource

The AS400 connector contains the IT Resource AS400 definition, which is used for either Target Reconciliation or Trusted Reconciliation.

The Oracle Identity Manager Connector Installer is used to create a new IT Resource based on the AS400 definition. The IT Resource `Configuration Lookup` parameter determines the reconciliation mode.

2.4.8.2 Specifying Values for the IT Resource Parameters

The Connector Installer allows you to create new IT Resources (type AS400) for both Target Reconciliation and Trusted Reconciliation.

Table 2–4 describes the parameters you must specify for a new IT Resource.

> **Note:**
>
> The ALL USERS group has INSERT, UPDATE, and DELETE permissions on the default IT resource. This is to ensure that end users can select the IT resource during request-based provisioning. If you create another IT resource, then you must assign INSERT, UPDATE, and DELETE permissions for the ALL USERS group on the IT resource.
>
> You must use the Administrative and User Console to configure the IT resource. Values set for the connection pooling parameters will not take effect if you use the Design Console to configure the IT resource.

To specify values for the parameters of the IT Resource:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1:

     Log in to the Administrative and User Console.
   - For Oracle Identity Manager release 11.1.2.*x* or later:

     Log in to Oracle Identity System Administration.
2. 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 Configuration region, click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   - Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
   - In the left pane under Configuration, click **IT Resource.**
4. On the Manage IT Resource page, select the type of IT Resource as AS400 in order to list the AS400 resources, 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, as described in Table Table 2–4.

Table 2–4 IT Resource Parameters

Parameter Name	Description
adminAccount	Administrator account name. Required. String. See Section 2.2.2.1, "Creating a Target System User Account for AS400 Connector Operations" for more information.
adminPassword	Administrator account password. Required. GuardedString. See Section 2.2.2.1, "Creating a Target System User Account for AS400 Connector Operations" for more information.
host	Hostname or IP address of the AS400 resource to connect to. Required. String.
useSSL	Boolean value that indicates whether to connect to the host using SSL. The default value is true. The useSSL property must be set to either true or false; it cannot be undefined.
Configuration Lookup	Name of the Lookup definition containing the configuration information. Values can be: ▪ `Lookup.Configuration.AS400` for Target Reconciliation ▪ `Lookup.Configuration.AS400.Trusted` for Trusted Reconciliation
Connector Server	Specifies the name of the Connector Server IT resource. The value for Oracle Identity Manager is Connector Server.

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

2.4.9 Configuring SSL for the Connector

This section describes how to configure Secure Sockets Layer (SSL) for the AS400 connector.

In summary, you must fetch the SSL certificate from the OS/400 target system and then import the certificate into the application server you are using.

Before you begin, consider these requirements:

- For the JDK requirements, see Section 1.1, "Certified Components." If necessary, set your *JAVA_HOME* environment variable to point to your specific JDK installation.
- SSL must be configured and enabled on the OS/400 server, and the Digital Certificate Manager must be started. For more information, see the IBM manual at the following location:

  `http://www-912.ibm.com/s_dir/slkbase.NSF/DocNumber/28604514`

To configure SSL for the AS400 connector, follow these steps:

1. Fetch the SSL certificate from the OS/400 target system:
   a. In a web browser, go to the Digital Certificate Manager on http://*OS400domain*:2001, where *OS400domain* is the OS/400 target system. Use the same user account and password that you use to access the target OS/400 system.
   b. In the left panel, select Create Certificate Authority.

      Or, if the Create Certificate Authority is not an option, select Install Local CA Certificate on Your PC.
   c. Select Install Certificate, and copy the certificate to a text file. For example: cert.txt
2. Determine the SSL keystore location on the application server you are using.

   For example, for Oracle WebLogic Server:
   a. Open the WebLogic Server Administration Console (http://*weblogicDomain*:*port*/console).
   b. Look for SSL configuration settings and specifically the name of the keystore. Sometimes, you will see the full path to the keystore, but other times you will see a name such as "DemoTrust" keystore with a path such as *WEBLOGIC_HOME*/server/lib/DemoTrust.jks.
3. Use the keytool -importcert command to add the certificate from Step 1 to the keystore for the specific AS400 connector application server.

   For example, for WebLogic Server:

   ```
   keytool -importcert -file path-to-certificate -alias arbitrary-alias
   -keystore <WEBLOGIC_HOME>/server/lib/DemoTrust.jks
   ```

   where:
   - *path-to-certificate* is the path to the certificate file you obtained in Step 1.
   - *arbitrary-alias* is a user-defined alias for identification of the certificate in the certificate store.
4. To verify presence of the certificate in the certificate store, use the `keytool -list -keystore` command.

2.4.10 Creating the IT Resource for the Connector Server

Perform the procedure described in this section only if you have installed the connector bundle in a Connector Server, as described in Section 2.3.2, "Deploying the Connector Bundle in a Connector Server." You must create a separate IT resource for the Connector Server.

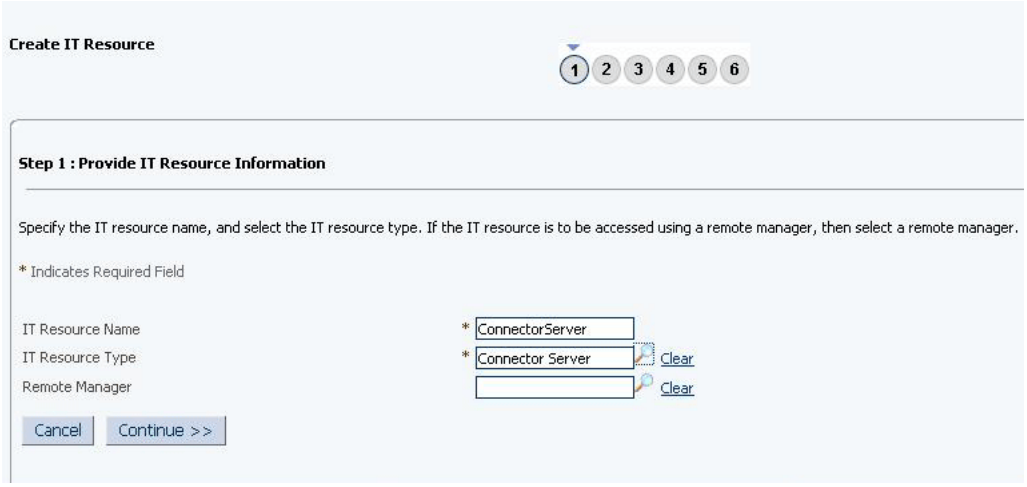
To create the IT resource for the Connector Server:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1:

     Log in to the Administrative and User Console.
   - For Oracle Identity Manager release 11.1.2.*x* or later:

     Log in to Oracle Identity System Administration.
2. 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 Configuration region, click **Create IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
   b. In the left pane under Configuration, click **IT Resource.**
   c. In the Manage IT Resource page, click **Create IT Resource.**
4. On the Step 1: Provide IT Resource Information page, perform the following steps:
   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.
5. Click **Continue**. Figure 2–2 shows the IT resource values added on the Create IT Resource page.

Figure 2–2 Step 1: Provide IT Resource Information



6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2–3 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2–3 Step 2: Specify IT Resource Parameter Values

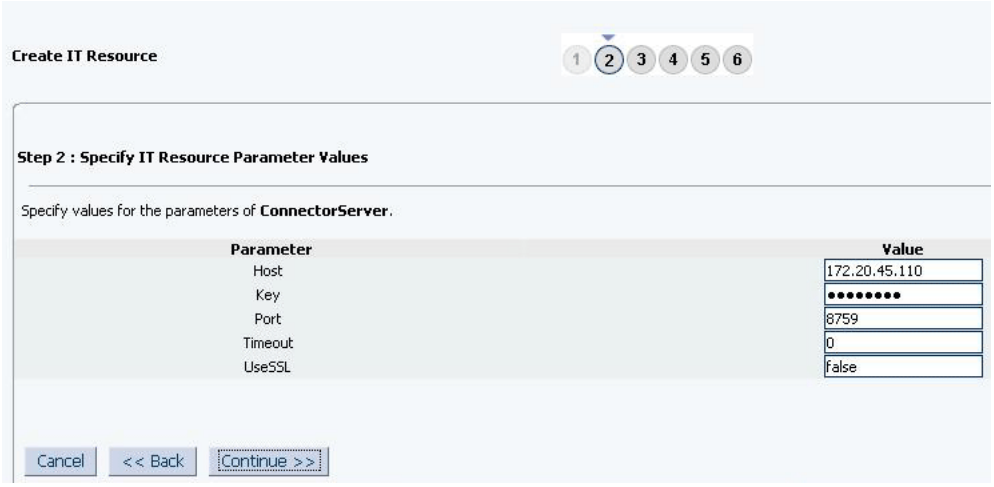


Table 2–5 provides information about the parameters of the IT resource.

Table 2–5 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `RManager`
Key	Enter the key for the Java connector server.

Table 2–5 (Cont.) Parameters of the IT Resource for the Connector Server

Parameter	Description
Port	Enter the number of the port at which the connector server is listening. Default value: `8759`
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `300`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, run the connector server by using the /setKey [*key*] option. The value of this key must be specified as the value of the Key IT resource parameter of the connector server.

7. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

   Note: This step is optional.

   If you want to assign groups to the IT resource and set access permissions for the groups, then:

   a. Click **Assign Group**.

   b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

   c. Click **Assign**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

   Note:

   - This step is optional.
   - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

   a. Click **Update Permissions**.

   b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

   c. Click **Update**.

9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

Note:

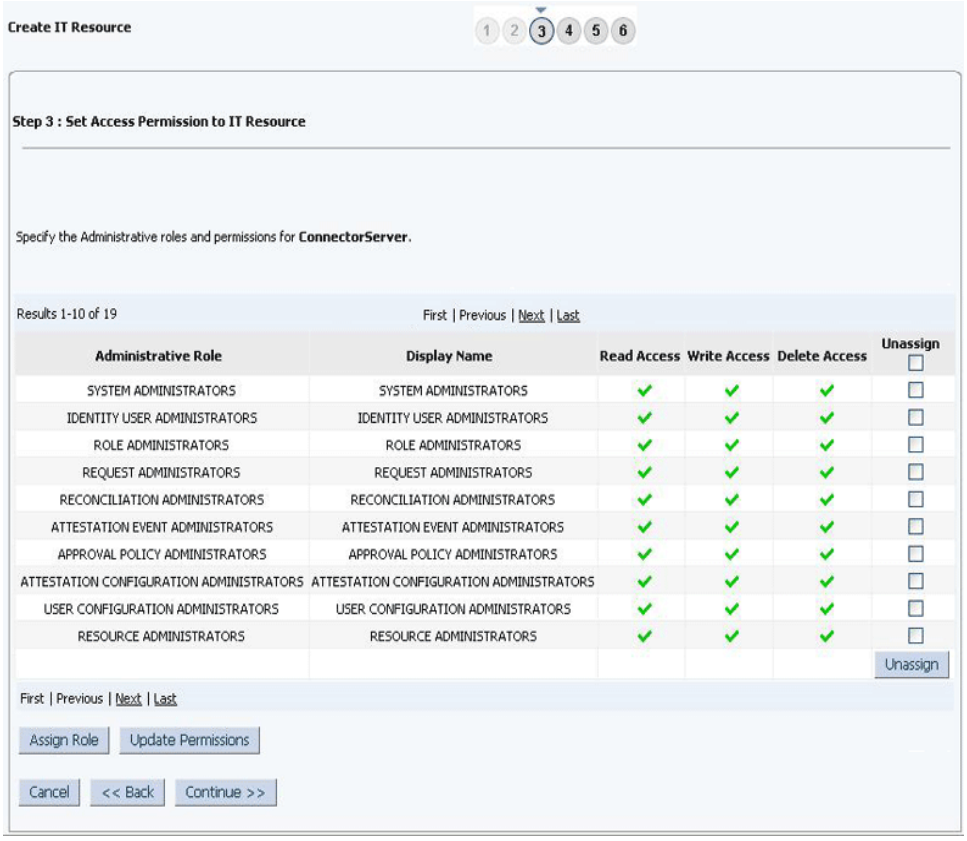
- This step is optional.
- You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

a. Select the **Unassign** check box for the group that you want to unassign.

b. Click **Unassign.**

10. Click **Continue**. Figure 2–4 shows the Step 3: Set Access Permission to IT Resource page.

Figure 2–4 Step 3: Set Access Permission to IT Resource



11. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

12. To proceed with the creation of the IT resource, click **Continue**. Figure 2–5 shows Step 4: Verify IT Resource Details page.

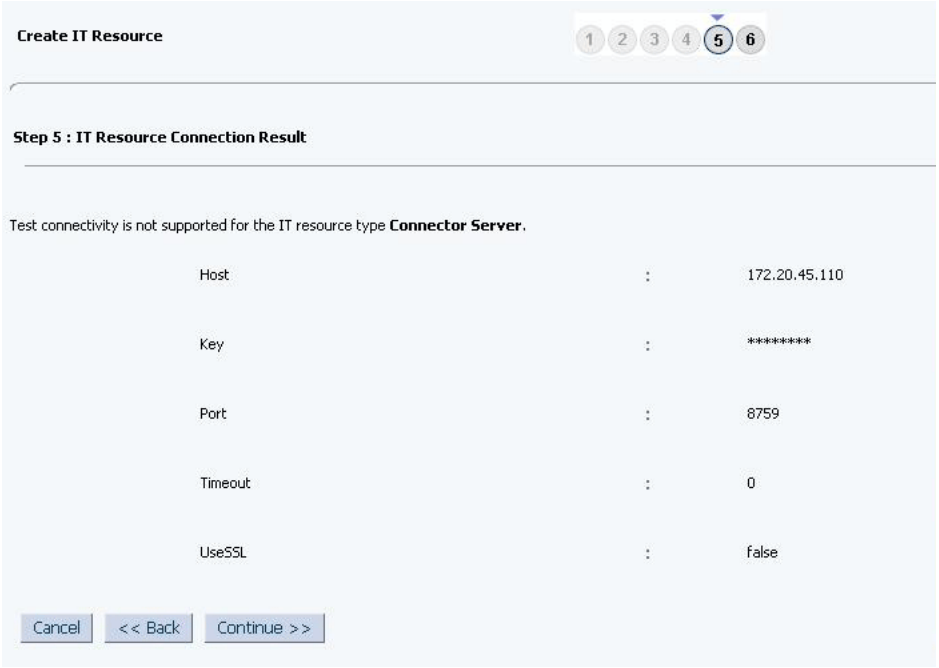
Figure 2–5 Step 4: Verify IT Resource Details

13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.

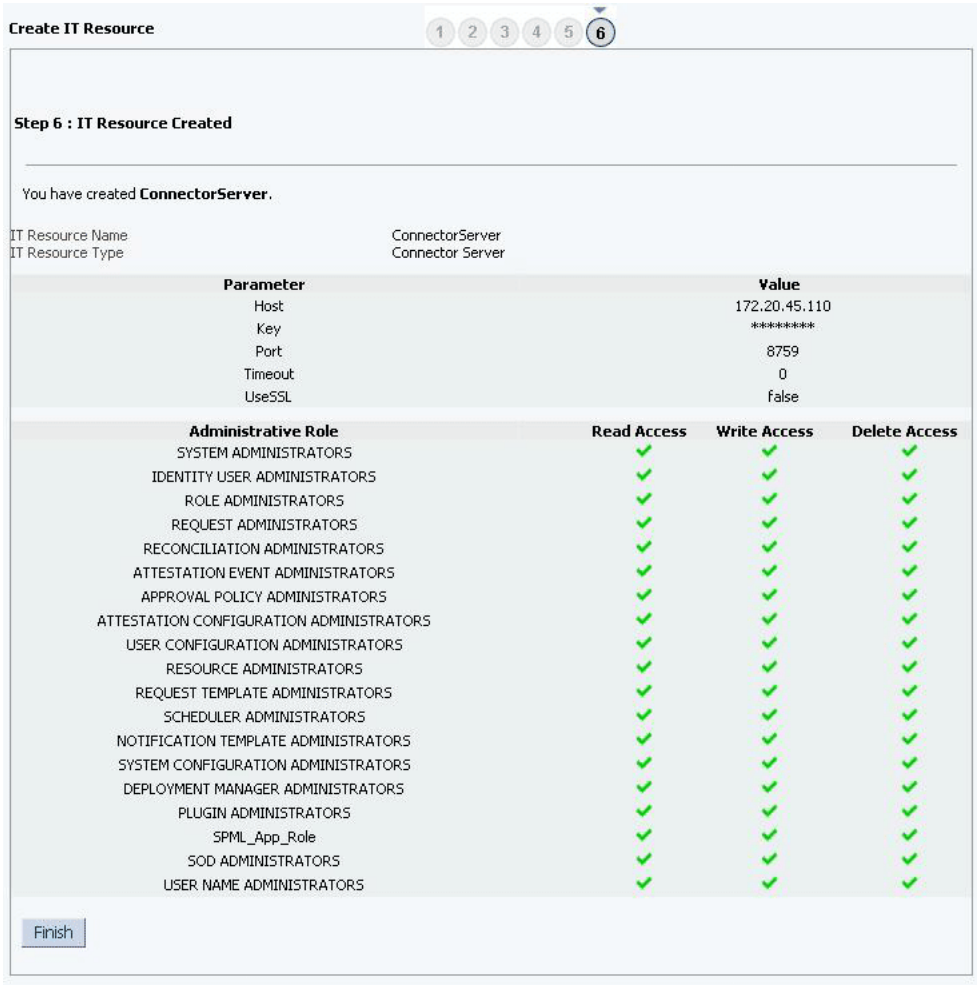
    Figure 2–6 shows the Step 5: IT Resource Connection Result page.

Figure 2–6 Step 5: IT Resource Connection Result



14. Click **Finish**. Figure 2–7 shows the IT Resource Created Page.

Figure 2–7 Step 6: IT Resource Created



2.4.11 Localizing Field Labels in UI Forms

Note: Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.*x* or later and you want to localize UI form field labels.

To localize field label that is added to the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open one of the following files in a text editor:
   - For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):

SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf

- For releases prior to Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0):

  SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf

6. Edit the BizEditorBundle.xlf file in the following manner:

   a. Search for the following text:

   ```
   <file source-language="en"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   b. Replace with the following text:

   ```
   <file source-language="en" target-language="LANG_CODE"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   In this text, replace LANG_CODE with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

   ```
   <file source-language="en" target-language="ja"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   c. Search for the application instance code. This procedure shows a sample edit for AS400 Account Name label. The original code is:

   ```
   <trans-unit
   id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
   ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
   rEO.UD_AS400CON_NAME__c_description']}">
   <source>Account Name</source>
   <target/>
   </trans-unit>
   <trans-unit
   id="sessiondef.oracle.iam.ui.runtime.form.model.AS400.entity.AS400EO.UD_AS4
   00CON_NAME__c_LABEL">
   <source>Account Name</source>
   <target/>
   </trans-unit>
   ```

   d. Open the resource file from the connector package, for example as400_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_AS400CON_NAME=\u30A2\u30AB\u30A6\u30F3\u30C8\u540D.

   e. Replace the original code shown in Step 6.c with the following:

   ```
   <trans-unit
   id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
   ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
   rEO.UD_AS400CON_NAME__c_description']}">
   <source>Account Name</source>
   <target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
   </trans-unit>
   <trans-unit
   ```

```
id="sessiondef.oracle.iam.ui.runtime.form.model.AS400.entity.AS400EO.UD_AS4
00CON_NAME__c_LABEL">
<source>Account Name</source>
<target>\u30A2\u30AB\u30A6\u30F3\u30C8\u540D</target>
</trans-unit>
```

f. Repeat Steps 6.a through 6.d for all attributes of the process form.

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace LANG_CODE with the code of the language to which you are localizing.

   Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

   See Also: Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager,* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Identity Manager.

2.5 Upgrading the Connector

You can perform the upgrade process while in production, and with no downtime. Your customizations will remain intact and the upgrade should be transparent to your users. Form field names are preserved from the legacy connector.

If you need to upgrade the AS400 connector from earlier versions to the current release 11.1.1.6.0, then the following is the summary of the procedure to upgrade the connector:

Note:

- Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- As a best practice, first perform the upgrade procedure in a test environment.

See Also: Upgrading Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information of these steps

1. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector.
2. Depending on the environment in which you are upgrading the connector, perform one of the following steps:
   - Staging Environment

     Perform the upgrade procedure by using the wizard mode.
   - Production Environment

Perform the upgrade procedure by using the silent mode.

3. Perform the postupgrade steps.
4. If you are using Oracle Identity Manager release 11.1.2.*x* or later, you must create a new UI form and attach it to an existing application instance to view the user-defined fields (UDFs or custom attributes).

   For more information about UDFs, see Configuring Custom Attributes in *Oracle Fusion Middleware Administering Oracle Identity Manager*.
5. Run the Form Version Control (FVC) utility to manage data changes on a form after an upgrade operation. To do so:

   a. In a text editor, open the fvc.properties file located in the *OIM_DC_HOME* directory and include the following entries:

   ```
   ResourceObject;AS400 User
   FormName;UD_AS400ADV
   FromVersion;v11
   ToVersion;v_11.1.1.6.0
   ParentParent;UD_AS400ADV_LDAPSERVER;UD_AS400ADV_SERVER
   ParentParent;UD_AS400ADV_UID;UD_AS400ADV_NAME
   ```

   b. The FromVersion (version of the earlier form) and the ToVersion (version of the new form mentioned during upgrade) can be viewed in the form designer of the design console. The following mappings have to be confirmed from the design console:

Existing Forms	New Forms
UD_SPECAUTH	UD_AS400CSP
UD_AS400ADV	UD_AS400CON
UD_SUPGRP	UD_AS400CSG

   c. Run the FVC utility. This utility is copied into the following directory when you install the design console:

   For Microsoft Windows:

   OIM_DC_HOME/fvcutil.bat

   For UNIX:

   OIM_DC_HOME/fvcutil.sh

   When you run this utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, and the logger level and log file location.

   See Also: Using the Form Version Control Utility in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the FVC utility

Note:

- After upgrading the connector, you must update the new bundle jar by adding the third party jar, jt400.jar (6.2), using the jar -uvf command. This command will ensure to keep the Manifest.mf file same as in the earlier version.
- The util400.jar file, which was required in the earlier version of the release is not required for the release 11.1.1.5.0 or later.

2.6 Postcloning Steps

You can clone the IBM AS400 connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

See Also: Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about cloning connectors and the steps mentioned in this section

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- Lookup Definition

  If the lookup definition contains the old lookup definition details, then you must modify it to provide the new cloned lookup definition names. If the Code Key and Decode values are referring the base connector attribute references, then replace these with new cloned attributes.

  For example, consider Lookup.AS400.UM.ProvAttrMap1 and UD_AS400CSG1 to be the cloned versions of the Lookup.AS400.UM.ProvAttrMap lookup definition and UD_AS400CSG child form, respectively.

  After cloning, the Lookup.AS400.UM.ProvAttrMap1 lookup definition contains Code Key entries that correspond to the fields of the old child form UD_AS400CSG. To ensure that the Code Key entries point to the fields of the cloned child form (UD_AS400CSG1), specify UD_AS400CSG1~Supplemental Group[Lookup] in the corresponding Code Key column.

- Scheduled Task

  You must replace the base connector resource object name in the scheduled task with the cloned resource object name. If the scheduled task parameter has any data referring to the base connector artifacts or attributes, then these must be replaced with the new cloned connector artifacts or attributes.

- Localization Properties

  You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

- IT Resource

  The cloned connector has its own set of IT resources. You must configure both the cloned IT resources, Active Directory and Connector Server, and provide the reference of the cloned Connector Server IT Resource in the cloned IBM AS400 IT resource. Ensure you use the configuration lookup definition of the cloned connector.

- Child Table

  As a result of a change in the name of the child table, you must modify the corresponding mappings for the child table operations to work successfully.

  To update the corresponding mappings, perform the following procedure:

  1. Log in to Design Console.
  2. Expand **Process Management,** and then double-click **Process Definition.**
  3. Search for and open the **AS400 User1** process form.
  4. Double-click the child table process task for the insert functionality. For example: **UD_AS400CSG1 Insert/ UD_AS400CSP1 Insert**

     The Editing Task window is displayed.
  5. On the Integration tab, select the row corresponding to the name of the child table, and then click **Map.**
  6. The Data Mapping for Variable window is displayed.
  7. Change the value in the Literal Value field to the cloned table name. For example, `UD_AS400CSG1`.
  8. Click **Save** and close the window.
  9. To change the mappings for the delete functionality, perform Steps 1 through 8 of this procedure with the following difference:

     While performing Step 4 of this procedure, instead of selecting the child table process task for the insert functionality, double-click the child table process task for the delete functionality.
  10. To change the mappings for the update functionality, perform Steps 1 through 8 with the following difference:

      While performing Step 4 of this procedure, instead of selecting the child table process task for the insert functionality, double-click the child table process task for the update functionality.

3

Using the Connector

This chapter is divided into the following sections:

- Section 3.1, "Scheduled Job for Lookup Field Synchronization"
- Section 3.2, "Configuring Reconciliation"
- Section 3.3, "Configuring Scheduled Jobs"
- Section 3.4, "Configuring Action Scripts"
- Section 3.5, "Configuring Provisioning in Oracle Identity Manager Release 11.1.1"
- Section 3.6, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"
- Section 3.7, "Uninstalling the Connector"

Note: These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

3.1 Scheduled Job for Lookup Field Synchronization

The AS400Connector Lookup Reconciliation scheduled job is used for lookup field synchronization. Values fetched by this scheduled task from the target system are populated in the `Lookup.AS400.Groups` lookup definition. Table 3–1 describes the attributes of this scheduled job. The procedure to configure scheduled jobs is described later in this guide.

Note: The target system allows you to use special characters in lookup fields. However, in Oracle Identity Manager, special characters are not supported in lookup definitions.

Table 3–1 Attributes of the AS400Connector Lookup Reconciliation Scheduled Task

Key	Value
IT Resource Name	Required name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `AS400`
Object Type	Name of the object type for the reconciliation run. Default value: `Group` Do not change the default value. `User` is the only supported object type.
Lookup Name	Name of the lookup definition into which values must be populated by the scheduled job. Default value: `Lookup.AS400.Groups` If you create a copy of the Lookup.AS400.Groups lookup definition, enter the name of that new lookup definition as the value of the Lookup Name attribute.
Code Key Attribute	Name of the connector attribute whose value is used to populate the Decode column of the Lookup.AS400.Groups lookup definition. Default value: `__UID__` Do not change the default value.
Decode Attribute	Name of the connector attribute whose value is used to populate the Code Key column of the Lookup.AS400.Groups lookup definition. Default value: `__NAME__` Do not change the default value.

3.2 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Section 3.2.1, "Limited Reconciliation"
- Section 3.2.2, "Reconciliation Scheduled Jobs"

3.2.1 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

Caution: If you are using filters in reconciliation as described in this section, be consistent and always use the same filters for delete and normal (trusted or target) reconciliation. By using the same filters, you will maintain consistency of the data and will ensure that you work with the same user base in all reconciliation operations.

With trusted delete reconciliation, make sure that you use the same filter you used in trusted reconciliation.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a Filter attribute (a scheduled task attribute) that allows you to use AS400 resource attributes to filter the target system records.

For detailed information about ICF Filters, see ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

Note: When referencing an OS/400 user profile in the "Filter" parameter for trusted reconciliation, the __UID__ attribute is not recognized.

Therefore, use the __NAME__ attribute when identifying an account for the OS/400 user profile.

3.2.2 Reconciliation Scheduled Jobs

Note: Attribute values are predefined in the connector XML file that you import. Specify values only for the attributes that you want to change.

The AS400 connector supports these scheduled jobs by default:

- AS400Connector Lookup Reconciliation
- AS400Connector Target User Delete Reconciliation
- AS400Connector Target User Reconciliation
- AS400Connector Trusted User Delete Reconciliation
- AS400Connector Trusted User Reconciliation

Common reconciliation parameters for all jobs are:

- Filter - optional filter to limit the number of reconciled accounts or to select specific set of users.
- IT Resource Name - required parameter specifying the name of IT Resource instance to recon.
- Object Type (constant) – User object class.
- Resource Object Name – constant parameter determining what OIM Resource Object to use for reconciliation.

3.3 Configuring Scheduled Jobs

To configure a scheduled job for the AS400 connector:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1:
     a. Log in to the Administrative and User Console.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   - For Oracle Identity Manager release 11.1.2.*x* or later:

a. Log in to Oracle Identity System Administration.

b. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see Managing Sandboxes in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

c. In the left pane, under System Management, click **Scheduler.**

2. Search for and open the scheduled job as follows:

   a. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

   b. 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.

3. On the page that is displayed, you can use any combination of the search options provided to locate a scheduled task. Click **Search** after you specify the search criteria.

   The list of scheduled tasks that match your search criteria is displayed in the search results table.

4. Select the link for the scheduled task from the list of scheduled tasks displayed in the search results table.

5. Modify the details of the scheduled job. To do so:

   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 Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

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

   On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

   Note: Attribute values are predefined in the connector XML file that is imported during the installation of the connector. Specify values only for the attributes that you want to change.

7. After specifying the attributes, 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 start, stop, or reinitialize the scheduler.

3.4 Configuring Action Scripts

Actions are scripts that you can configure to run before or after `create`, `update`, and `delete` provisioning operations. For example, you can configure a script to run before every user creation.

The AS400 connector supports the **OS/400 Command Language** and target: **Resource**.

The target indicates where the script is executed. For the target Resource, the script is executed on the computer where the target resource is running (and is typically interpreted by the target computer).

To configure the action:

1. Log in to the Design Console.
2. Search for and open the **Lookup.AS400.UM.Configuration** lookup definition.
3. Add the following new values:
   - **Code Key**: Before Create Action Language
   - **Decode**: Enter the scripting language of the script you want to execute. The AS400 connector supports the OS/400 Command Language. Specify the value as "OS/400 CL."

     Note: The only value supported for the AS400 connector is "OS/400 CL."
4. Add these new values:
   - **Code Key**: Before Create Action File
   - **Decode**: Enter the full path to the file containing the script to be executed. Oracle Identity Manager must be able to access this file.

     For example, the following command in a file sets the value of the TEXT attribute to the text specified by 'new text description' for a new account:

     ```
     CHGUSRPRF USRPRF($__NAME__$) TEXT('new text description')
     ```
5. Add these new values:
   - **Code Key**: Before Create Action Target
   - **Decode**: Allowed value is `Resource`.
6. Save the lookup.

Now, this action will be executed every time you create a user. You must configure these values for each action you want to execute.

3.5 Configuring Provisioning in Oracle Identity Manager Release 11.1.1

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, 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 3.5.3, "Switching Between Request-Based Provisioning and Direct Provisioning."

The following are types of provisioning operations:

- Direct provisioning
- Request-based provision

> **See Also:** See Manually Completing a Task in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

- Section 3.5.1, "Direct Provisioning"
- Section 3.5.2, "Request-Based Provisioning"
- Section 3.5.3, "Switching Between Request-Based Provisioning and Direct Provisioning"

3.5.1 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:
   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:
   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. On the user details page, click the **Resources** tab.
5. 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.
6. On the Step 1: Select a Resource page, select **AS400 User** from the list and then click **Continue**.
7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. On the Step 5: Provide Process Data for AS400 Connector User page, enter the details of the account that you want to create on the target system and then click **Continue**.
9. (Optional) On the Step 5: Provide Process Data for Special Authorities page, specify the special authorities for the user on the target system and then click **Continue**.

10. (Optional) On the Step 5: Provide Process Data for Supplemental Group page, search for and select a supplemental group for the user on the target system and then click **Continue**.
11. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
12. The "Provisioning has been initiated" message is displayed. Close the window displaying this message.
13. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.2 Request-Based Provisioning

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 3.5.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.5.2.2, "Approver's Role in Request-Based Provisioning"

3.5.2.1 End User's Role in Request-Based Provisioning

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

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 **AS400 User**, 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.

3.5.2.2 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.

3.5.3 Switching Between Request-Based Provisioning and Direct Provisioning

Note: It is assumed that you have performed the procedure described in Section 2.4.4, "Enabling Request-Based Provisioning."

To switch from request-based provisioning to direct provisioning:

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 **AS400 User Process Form** 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 **AS400 User** resource object.

c. Deselect the **Self Request Allowed** check box.

d. Click the Save icon.

To switch from direct provisioning back to request-based provisioning:

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 **AS400 User Process Form** 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 **AS400 User** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the Save icon.

3.6 Configuring Provisioning in Oracle Identity Manager Release 11.1.2

To configure provisioning operations in Oracle Identity Manager release 11.1.2:

Note: The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance, and then click **Checkout.**
5. Specify value for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

3.7 Uninstalling the Connector

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oralce Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

> **Note:** From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* guide for information about managing lookups by using the Form Designer in the Oracle Identity Manager System Administration console.

4.1 Adding Target System Attributes

Adding target system attributes includes the following subsections:

> **Note:** If you add an attribute with a Date type field, make sure that you add the `[Date]` suffix in the Lookup definition code key.
>
> For example, if you add _LAST_PASSWORD_CHANGE_DATE_, when you make changes in the code key for Lookup.AS400.UM.ReconAttrMap or Lookup.AS400.UM.ProvAttrMap, specify the attribute as:
>
> `_LAST_PASSWORD_CHANGE_DATE_[Date]`

4.1.1 Adding Target System Attributes for Provisioning

By default, the attributes listed in Section 1.5.1, "User Attributes for Target Resource Reconciliation and Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning by performing these steps.

Note: In this section, the term "attribute" refers to the identity data fields that store user data.

Do not repeat steps that you have performed as part of the procedure described in Section 4.1.2, "Adding Target System Attributes for Target Reconciliation".

To add a target system attribute for provisioning, follow these steps:

1. Add a new form field. To add a new field to the Process form:
   a. Open the Form Designer form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
   b. Query for the UD_AS400CON form.
   c. Click **Create New Version**. The Create a New Version dialog box is displayed.
   d. In the Label field, enter the name of the version.
   e. Click **Save** and close the dialog box.
   f. From the Current Version box, select the version name that you entered in the Label field in Step 4.
   g. On the Additional Columns tab, click **Add**.
   h. Specify the new field name and other values.
   i. Click **Save**.
   j. Click **Make Version Active** to make the new form field visible to the user.

      Now, if you go to Oracle Identity Manager and try to provision a new user to AS400, you should see the new form field. Next, you must add the new form field to the Provisioning Mapping Lookup.
2. Add the new field to the Provisioning Mapping Lookup. After creating a new form field, you must add that field to the Provisioning Mapping Lookup, as follows:
   a. Expand **Administration** and then double-click **Lookup Definition**.
   b. In the Lookup Definition window, search for **AS400**.

      The Design Console returns Lookup.AS400.UM.ProvAttrMap.
   c. Select the Lookup Definition Table tab, and select **Lookup.AS400.UM.ProvAttrMap**.

      The Lookup Code Information tab maps the Oracle Identity Manager form field names and the AS400 Identity Connector attributes. Where the Code Key column contains the Oracle Identity Manager field labels and the Decode column contains the attribute names supported by the AS400 identity connector.

d. Add a new record for the new form field. Type the new form field name into the Code Key column and type the AS400 identity connector attribute name into the Decode column.

e. Click **Save**.

Now, when you create a new AS400 user, the connector will get the new attribute as part of the create operation.

At this point, the process task only handles creates. Next, you must change the process task to also handle updates. Instructions are described in the next steps.

3. Change the process task to handle updates, as follows:

a. In the Design Console, expand **Process Management** and then double-click **Process definition**.

b. Search for and select process **AS400 User.**

c. In the Task column, look for an update task that is similar to the one you want to add and select that entry.

d. Click **Add**.

e. In the Creating New Task dialog, select the General tab and enter a Task Name and a Task Description.

The Task Name is important because it will be the form name field. Be sure to include the event you want the task to handle. For example, if you add the Building field for provisioning, then add the Building Updated task. Now, this update event will be triggered when the Building field is updated.

f. In the Task Properties section, set the following properties as noted:

-Conditional: Enabled

-Required for Completion: Disabled

-Disable Manual Insert: Disabled

-Allow Cancellation while Pending: Enabled

-Allow Multiple Instances: Enabled

You do not have to change any of the remaining properties.

g. Save your changes.

h. To add an Event Handler, select the Integration tab, and then click **Add**.

i. When the Handler Select dialog box displays, select Adapter as the handler type and then perform the following steps:

Select adapter **adpAS400CONNECTORUPDATEATTRIBUTEVALUE** and click **Save**.

Map all of the variables that are configured for the event adapter.

In the Adapter Variables section, double-click a variable name to open the Edit Data Mapping For Variable dialog box. Specify the following values for each variable in turn. Be sure to save your changes after each mapping.

Variable Name	Map To	Qualifier	Literal Value
itResourceFieldName	Literal	String	UD_AS400CON_SERVER

Variable Name	Map To	Qualifier	Literal Value
processInstanceKey	Process Data	Process Instance	
Adapter return value	Response Code		
objectType	Literal	String	User
attrName	Literal	String	Enter your new label

j. Save and close the Creating New Task dialog.

k. Check the Task column on the Process Definition tab to verify that the new process task is listed. Also verify that the new form field is available and working in Oracle Identity Manager.

4. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.4.1.2, "Creating a New UI Form" and Section 2.4.1.6, "Updating an Existing Application Instance with a New Form" for the procedures.

4.1.2 Adding Target System Attributes for Target Reconciliation

By default, the attributes listed in Section 1.5.1, "User Attributes for Target Resource Reconciliation and Provisioning" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for target reconciliation as described in this section.

Note:

- Perform this procedure only if you want to add new target system attributes for reconciliation.
- In the following steps, a new attribute called BUILDING will be added, its connector attribute name is BUILDING, and the form field name is Building. Names are case-sensitive.

To add a new target system attribute for target reconciliation, follow these steps:

1. 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 **AS400 User** 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 that is the name of the new Attribute on your Form.

      For example: Building

   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. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.

2. If a corresponding field does not exist in the process form, then add a new column in the process form, as follows:

a. Open the Form Designer form. This form is in the Development tools folder.

b. Query for the UD_AS400CON form.

c. Click **Create New Version**. The Create a New Version dialog box is displayed.

d. In the Label field, enter the name of the version.

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

f. From the Current Version box, select the version name that you entered in the Label field in Step 3.

g. On the Additional Columns tab, click **Add**.

h. In the Name field, enter the name of the data field and then enter the other details of the field.

Note: Repeat Steps g and h if you want to add more attributes.

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

3. 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 **AS400 User** 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 added in Step 2e.

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.

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

4. Go to the reconciliation lookup, Lookup.AS400.UM.ReconAttrMap, and add a new record for the new attribute using the following values:

- Code Key - Name of the reconciliation field
- Decode - Name of the AS400 attribute

5. In the Design Console, regenerate the reconciliation profile for the Resource Object.

6. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.4.1.2, "Creating a New UI Form" and Section 2.4.1.6, "Updating an

Existing Application Instance with a New Form" for the procedures.

4.1.3 Adding Target System Attributes for Trusted Reconciliation

By default, the attributes listed in Section 1.5.1, "User Attributes for Target Resource Reconciliation and Provisioning" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for trusted reconciliation as described in this section.

Note:

- Perform this procedure only if you want to add new target system attributes for reconciliation.
- In the following steps, a new attribute called BUILDING will be added, its connector attribute name is BUILDING, and the form field name is Building. Names are case-sensitive.

To add a new target system attribute for trusted reconciliation, follow these steps:

1. 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 **AS400 Trusted User** 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 that is the name of the new Attribute on your Form.

      For example: Building
   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. Click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
2. If a corresponding field does not exist in the process form, then add a new column in the process form, as follows:
   a. Open the Form Designer form. This form is in the Development tools folder.
   b. Query for the UD_AS400CON form.
   c. Click **Create New Version**. The Create a New Version dialog box is displayed.
   d. In the Label field, enter the name of the version.
   e. Click **Save** and close the dialog box.

f. From the Current Version box, select the version name that you entered in the Label field in Step 3.

g. On the Additional Columns tab, click **Add**.

h. In the Name field, enter the name of the data field and then enter the other details of the field.

Note: Repeat Steps g and h if you want to add more attributes.

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

3. 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 **AS400 Trusted User** 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 added in Step 2e.

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.

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

4. Go to the reconciliation lookup, Lookup.AS400.UM.ReconAttrMap.Trusted, and add a new record for the new attribute using the following values:

- Code Key - Name of the reconciliation field
- Decode - Name of the AS400 attribute

5. If you are using Oracle Identity Manager release 11.1.2.*x* or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.4.1.2, "Creating a New UI Form" and Section 2.4.1.6, "Updating an Existing Application Instance with a New Form" for the procedures.

4.2 Configuring Validation and Transformation

You can configure validation for provisioned and reconciled single-valued data according to your requirements. You can also configure transformation, but it is only supported for reconciliation.

Instructions for configuring validations and transformations are described in the following sections:

- Section 4.2.1, "Configuring Validation for Provisioning"
- Section 4.2.2, "Configuring Validation for Reconciliation"
- Section 4.2.3, "Configuring Reconciliation Transformation"

4.2.1 Configuring Validation for Provisioning

To configure validation for provisioned data, follow these steps:

1. Write some custom Java class code to implement the `oracle.iam.connectors.common.validate.Validator` interface. For example:

```
package com.validationexample;
import oracle.iam.connectors.common.ConnectorException;
import oracle.iam.connectors.common.validate.Validator;

import java.util.HashMap;

public class MyValidator implements Validator {
    public boolean validate(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {

        /* You must write code to validate attributes. Parent
                 * data values can be fetched by using hmUserDetails.get(field)
                 * For child data values, loop through the
                 * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")
                 * Depending on the outcome of the validation operation,
                 * the code must return true or false.
                 */
        /*
        * In this sample code, the value "false" is returned if the field
        * contains the number sign (#). Otherwise, the value "true" is
        * returned.
        */
        boolean valid = true;
        String sFirstName = (String) hmUserDetails.get(sField);
        for (int i = 0; i < sFirstName.length(); i++) {
            if (sFirstName.charAt(i) == '#') {
                valid = false;
                break;
            }
        }
        return valid;

    }
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to the Oracle Identity Manager database.

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   - For Microsoft Windows: OIM_HOME\server\bin\UploadJars.bat
   - For UNIX: OIM_HOME/server/bin/UploadJars.sh

   Note: Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. Log in to the Design Console.
5. Search for and open the `Lookup.AS400.UM.ProvValidation` (or create another custom name) lookup definition.

   Note: If you cannot find the `Lookup.AS400.UM.ProvValidation` lookup definition, create a new lookup.

6. In the Code Key column, enter the resource object field name that you want to validate.
7. In the Decode column, enter the class name.

   For example, com.*validationexample.MyValidator*.
8. Save your changes to the lookup definition.
9. Search for and open the `Lookup.AS400.UM.Configuration` lookup definition.
10. In the Code Key column, enter **`Provisioning Validation Lookup`**.
11. In the Decode column, enter **`Lookup.AS400.UM.ProvValidation`** or enter the name of the lookup you created in step 3.

4.2.2 Configuring Validation for Reconciliation

The steps for configuring reconciliation validation are the same as the steps described in Section 4.2.1, "Configuring Validation for Provisioning", except that the Code Key in step 8 must be **`Recon Validation Lookup`**.

4.2.3 Configuring Reconciliation Transformation

You can configure transformation of reconciled single-valued user data according to your requirements. For example, you could use `First Name` and `Last Name` values to create a value for the **Full Name** field in Oracle Identity Manager.

To configure the reconciliation transformation:

1. Write a custom Java class to implement the Transformation interface. For example:

```
package com.transformationexample;

  import oracle.iam.connectors.common.transform.*;
  import java.util.HashMap;

  public class MyTransformer implements Transformation {

    public Object transform(HashMap hmUserDetails, HashMap
         hmEntitlementDetails,String sField) {
      String sFirstName= (String)hmUserDetails.get("First Name");
      String sLastName= (String)hmUserDetails.get("Last Name");
      String sFullName=sFirstName+"."+sLastName;
      return sFullName;
   }
}
```

2. Create a JAR file to hold the Java class.
3. Copy the JAR file to the Oracle Identity Manager database.

   Run the Oracle Identity Manager Upload JARs utility to post the JAR file to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   - For Microsoft Windows: OIM_HOME\server\bin\UploadJars.bat
   - For UNIX: OIM_HOME/server/bin/UploadJars.sh

   Note: Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.
4. Log in to the Design Console.
5. Search for and open the **Lookup.AS400.UM.ReconTransformation** (or create another custom name) Lookup definition.

   Note: If you cannot find the Lookup.AS400.UM.ReconTransformation lookup definition, create a new lookup.

6. In the Code Key column, enter the resource object field name you want to transform (`AS400 User` for target reconciliation and `AS400 Trusted User` for trusted reconciliation).
7. In the Decode column, enter the class name.

   For example, com.*transformationexample.MyTransformer*.
8. Save the changes to the lookup definition.
9. Search for and open the `Lookup.AS400.UM.Configuration` lookup definition.
10. In the Code Key column, enter **`Recon Transformation Lookup`**.
11. In the Decode column, enter **`Lookup.AS400.UM.ReconTransformation`** or enter the name of the lookup you created in step 3.

4.3 Configuring Connection Pooling

The AS400 connector uses Identity Connector Framework (ICF) connection pooling.

Connection pooling involves the management of connector instances, so that an OS/400 connection does not have to be created each time an operation is executed. For most applications, the default connection pooling setup should be sufficient. However, the fine-tuning of connection pooling can help to increase throughput, if maximum performance is a concern.

To set up connection pooling for the AS400 connector, add the entries shown in Table 4–1 to the Lookup.Configuration.AS400 definition using the Oracle Identity Manager Design Console.

Table 4–1 Connection Pooling Parameters

Parameter	Type and Values	Description
Pool Max Idle	Integer, greater than or equal to 0. Should be greater than Pool Min Idle.	Maximum number of idle connector instances.
Pool Max Size	Integer, greater than or equal to 0.	Maximum number of connector instances in the pool.
Pool Max Wait	Integer, greater than or equal to 0.	Maximum time in milliseconds to wait if the pool is waiting for a free connector instance to become available. Zero means don't wait.
Max Pool Evict Time	Integer, greater than or equal to 0.	Maximum time in milliseconds to wait before evicting an idle connector instance.
Pool Min Evict Idle Time	Integer, greater than or equal to 0.	Minimum time in milliseconds to wait before evicting an idle connector instance.
Pool Min Idle	Integer, greater than or equal to 0. Should be less than Pool Max Idle.	Minimum number of idle connector instances.

4.4 Modifying Field Lengths on the Process Form

You might want to modify the lengths of fields (attributes) on the process form. For example, if you use the Japanese locale, you might want to increase the lengths of process form fields to accommodate multibyte data from the target system.

To modify the length of a field on the process form, follow these steps:

1. Log in to the Design Console.
2. Expand **Development Tools**, and double-click **Form Designer**.
3. Search for and open the **UD_AS400** process form.
4. Click **Create New Version**.
5. Enter a label for the new version, click the Save icon, and then close the dialog box.
6. From the **Current Version** list, select the version that you create.
7. Modify the length of the required field.
8. Click the Save icon.
9. Click **Make Version Active**.
10. Define the connector. If you are planning to perform any of the other procedures described in this chapter, perform those procedures and then define the connector. See Section 4.6, "Defining the Connector" for more information.

4.5 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

You can use access policies to manage multiple installations of the target system.

Note: If you want to create copies of all the objects that constitute the connector, then see Cloning Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4.6 Defining the Connector

By using the Administrative and User Console, you can define a customized or reconfigured connector. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

A connector is automatically defined when you install it using the Install Connectors feature or when you upgrade it using the Upgrade Connectors feature. You must manually define a connector if:

- You import the connector by using the Deployment Manager.
- You customize or reconfigure the connector.
- You upgrade Oracle Identity Manager.

The following events take place when you define a connector:

- A record representing the connector is created in the Oracle Identity Manager database. If this record already exists, then it is updated:
- The status of the newly defined connector is set to Active. In addition, the status of a previously installed release of the same connector automatically is set to Inactive.

See Defining Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the procedure to define connectors.

4.7 Enabling Ad-Hoc Linking

During trusted source reconciliation of a new user, whose account is not existing in Oracle Identity Manager, an event is generated for that user by throwing a "no match found" error. You can link this new user to any of the user already existing in Oracle Identity Manager using Ad-Hoc linking.

To enable Ad-Hoc linking for a user:

1. Log in to Design Console.
2. Go to Development Tools, Form Designer.
3. In the Table Name field, enter `UD_AS400CON` and click **Preview Form** to open the form.
4. Click **Create New Version**.

5. Click on the **Properties** tab.
6. Under the Password (PasswordField) property, set the Required Property Value to `False`.
7. Click **Save**.
8. Click **Make Version Active**.

5

Troubleshooting

This chapter provides solutions to problems you might encounter after you deploy the AS400 connector.

5.1 Troubleshooting

To get relevant information about the AS400 connector and the Identity Connector Framework (ICF), look for the "identityconnectors" and "as400" keywords in the Oracle Identity Manager server log.

Table 5–1 provides solutions to problems you might encounter with the AS400 connector.

Table 5–1 Troubleshooting for the AS400 Connector

Problem	Solution
Provisioning did not succeed, and the user is in the "Provisioning" state.	Look for the error message under the "Show Resource History" button. Double-check that the host, adminUser, and adminPassword are correct in your AS400 IT Resource. Try to verify the correctness of these values by logging in to OS/400 system. From Windows use IBM iNavigator, or the tn5250 console from Unix.
A scheduled task fails.	Make sure the IT Resource parameter is defined on the scheduled task. If a Filter is defined, check its correctness based on the rules as in Section 3.2.1, "Limited Reconciliation."
The update of an attribute failed.	You might see this message under "Show Resource History" button, when you click on the "*Operation* Rejected" entry. The update of an attribute can fail because: ▪ A required value is missing. ▪ The value is present, but it is not a valid OS/400 attribute. See Section 1.5.1, "User Attributes for Target Resource Reconciliation and Provisioning." ▪ You are unable to connect to the resource because either the IT Resource is not configured correctly or the physical connection is down.

Table 5–1 (Cont.) Troubleshooting for the AS400 Connector

Problem	Solution
You are unable to update the Supplemental Group attribute.	To populate the Supplemental Group attribute, first define a primary group (Group Profile).
Trusted reconciliation fails because some attributes are missing.	If an OS/400 account is created manually using the OS/400 Command Language (CRTUSRPRF command), a Directory Entry is not created for the account. When trusted reconciliation is run, some attributes such as First Name, Last Name, and Login are required for a successful reconciliation. If any attributes are missing, the reconciliation fails. Because the OS/400 account does not have an OS/400 Directory Entry, it does not have the required values. Therefore, the trusted reconciliation is unsuccessful. Create an OS/400 Directory Entry for the user account using the OS/400 Command Language. Or, use the Transformation feature and write custom Java code that will look up the attributes in the directory (for example, an LDAP directory) and fill-in the required attributes.
Trusted reconciliation fails because of a problem with matching rule.	Ensure that the value of the Configuration Lookup parameter of the IT resource is set to `Lookup.Configuration.AS400.Trusted`. See Table 2–4 for information about the Configuration Lookup IT resource parameter.

6

Known Issues

This chapter describes the following known issues associated with this release of the AS400 connector:

- **Bug 11671704**

  The UID attribute is a unique number that identifies a user on the OS/400 target system. In Oracle Identity Manager, the UID attribute is not part of the default user form. You can add the UID to your user form, process as read-only attribute. For information about adding attributes, see Section 4.1.3, "Adding Target System Attributes for Trusted Reconciliation."

  Workaround:

  To update the UID attribute, use the OS/400 Command Language (CHGUSRPRF command).

- **Bug 12635601**

  Provisioning User with shortened path (*LIBRARY_FOLDER/LIBRARY*) value for INLMNU, INLPGM, ATNPGM, OUTQ, and SRTSEQ fails with com.ibm.as400.access.IllegalPathNameException.

  Workaround:

  When you create the OS/400 account for the OIM user, specify the fully-qualified path for these attributes. For example, for the job description attribute:

  Value for the attribute JOBD in short path:

  QGPL/QDFTJOBD

  The same value in fully qualified path:

  /QSYS.LIB/QGPL.LIB/QDFTJOBD.JOBD

A

Policies for OS/400 Accounts Migration

The AS400 connector has extended a number of supported attributes, as compared to previous releases of the OS/400 Oracle Identity Manager connector. Some of the new attributes (for example, First Name and Last Name) are stored in an OS/400 Directory Entry object. Directory Entries were not used by previous releases of the connector.

Sources of OS/400 accounts without Directory Entries include:

- An account provisioned by the legacy OS/400 Oracle Identity Manager connector
- An account created manually by an OS/400 administrator

The AS400 connector has the following policy for the creation of a Directory Entry:

- A new OS/400 account is provisioned.
- An OS/400 account attribute is updated.

The AS400 connector does not create a Directory Entry if a search or reconciliation operation is performed.

The AS400 connector uses two objects to save OS/400 account attributes: User Profile and Directory Entry. These entities are mapped as follows on connector operations:

- Create operation: New users created by the connector will have both a Directory Entry and a User Profile.
- Delete operation: Legacy users without a Directory Entry will be logged in with a warning for a delete operation.
- Search operation: For legacy users without a Directory Entry, empty attribute values will be returned (if attributes of a Directory Entry are requested by the search operation).
- Update operation: If the Directory Entry is missing for an account, the connector will create an empty Directory Entry for the OS/400 account.

Index

R

S

T

U

V