Oracle® Identity Manager

Connector Guide for RSA Authentication Manager

Release 9.0.4

E11207-08

November 2010

Oracle Identity Manager Connector Guide for RSA Authentication Manager, Release 9.0.4

E11207-08

Primary Author: Lyju Vadassery

Contributing Authors: Devanshi Mohan, Alankrita Prakash

Contents

3 Configuring the Connector

4 Known Issues

Index

Preface

This guide provides information about Oracle Identity Manager Connector for RSA Authentication Manager.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for RSA Authentication Manager.

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/support/contact.html` or visit `http://www.oracle.com/accessibility/support.html` if you are hearing impaired.

Related Documents

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

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

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

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

Documentation Updates

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

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

Conventions

The following text conventions are used in this document.

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

What's New in the Oracle Identity Manager Connector for RSA Authentication Manager?

This chapter provides an overview of the updates made to the software and documentation for the RSA Authentication Manager connector in release 9.0.4.12.

Note: Release numbers from 9.0.4.4.through 9.0.4.11 have not been used.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

  These include major changes made to the connector documentation. These changes are not related to software updates.

See Also: *Oracle Identity Manager Release Notes*

Software Updates

The following sections discuss updates made in the connector:

- Software Updates Up To Release 9.0.4.1
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.12

Software Updates Up To Release 9.0.4.1

The following software updates have been made up to release 9.0.4.1 of the connector:

- In this release, you can reconcile new target system resource object fields. The fields are mentioned in the "Reconciled Resource Object Fields" section on page 1-3.
- In this release, the list of fields for which you can specify values RSA Authentication Manager user provisioning is updated. The updated list of fields is in the "RSA Authentication Manager User Provisioning" section on page 1-5.

- In this release, you can indicate the status of the users that need to be deleted while performing delete reconciliation in trusted mode. This is done by specifying the value of the `TrustedDeleteReconObjectStatusList` scheduled task attribute.

  The `TrustedDeleteReconObjectStatusList` scheduled task attribute is described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3.

- The CustomReconQuery reconciliation query condition is moved from IT resources to Task Scheduler. For information about CustomReconQuery, see the "Limited Reconciliation" section on page 3-1.

- In this release, you can configure the separator while specifying multiple group names as the value of `CustomReconQuery`. This is done by specifying the value of the `GroupTokenizerForCustomReconQuery` scheduled task attribute, which is discussed in the following sections:

  - "Limited Reconciliation" section on page 3-1
  - "Configuring the Reconciliation Scheduled Tasks" section on page 3-3

- New scheduled task attributes are defined in this release of the connector that are discussed in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3.

- In this release, the list of adapters that are imported into Oracle Identity Manager when you import the connector XML file is updated. See the "Compiling Adapters" section on page 3-8.

- In the "Running Connector Tests" section on page 4-1, the following default attribute values are added:

  - `isTemporaryUserstartDate`
  - `startTime`
  - `endDate`
  - `endTime`

- In Chapter 4, "Known Issues" on page 4-1, the following known issues are added:

  - When creating a temporary user during provisioning, you can specify start time or end time in hours, but you can not provide the start time or end time in hours and minutes. This is because the target system API accepts these values in hours (0-23) only. If you specify the time in hours and minutes, the API will throw the error. To avoid providing the time in hours and minutes format from the UI, a lookup is provided that has values from 0 through 23 for start time and end time.
  - To synchronize reconciliation of start time or end time with provisioning, if the target system start time or end time as 0-0:59, then it is rounded off to 0. The reconciliation of start time or end time is matched with the start time and end time of provisioning. If the target system start time or end time is in hour and minute, then the start time or end time value is rounded off. For example, 1 hour and 59 minutes is rounded off to 1 hour.
  - RSA Authentication Manager connector cannot be configured with multiple schedulers to reconcile users from RSA Authentication Manager because RSA ACE API is not thread safe. This means that the fields of an object or class do not maintain a valid state if multiple threads are running.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Support for New Target System Version
- Resolved Issues in Release 9.0.4.2

Support for New Target System Version

RSA Authentication Manager 6.1.2 running on Solaris 9 has been added to the list of certified target system versions. See "Step 1: Verifying Deployment Requirements" for information about the full list of certified target system versions.

Resolved Issues in Release 9.0.4.2

The following is an issue resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
8317806	During target resource reconciliation, even user records that had not been modified were fetched into Oracle Identity Manager.	This issue has been resolved. During target resource reconciliation, only newly created and modified user records are fetched into Oracle Identity Manager.

Software Updates in Release 9.0.4.3

The following are software updates in release 9.0.4.3:

- Using the Connector Installer
- Support for New Target System Version
- Resolved Issues in Release 9.0.4.3

Using the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See the "Installing the Connector on Oracle Identity Manager Release 9.1.0.x and Release 11.1.1" section for more information.

Support for New Target System Version

RSA Authentication Manager 6.1.2 running on Solaris 10 has been added to the list of certified target system versions. See "Step 1: Verifying Deployment Requirements" for information about the full list of certified target system versions.

Resolved Issues in Release 9.0.4.3

The following issues are resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
5554933	During trusted source reconciliation, two reconciliation events were created for each user record fetched from the target system.	This issue has been resolved. Only a single reconciliation event is created for each user record fetched from the target system.
8517925	Delete user task was rejected in delete user reconciliation.	This issue has been resolved. The delete user task is working as expected.
5180636	Null response received after resetting the Pin.	This issue has been resolved.

Bug Number	Issue	Resolution
8525566	Delete reconciliation fetched records that were not deleted.	This issue has been resolved.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

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

Support for New Oracle Identity Manager Release

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

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

Support for Request-Based Provisioning

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

See "Configuring Oracle Identity Manager Release 11.1.1 for Request-Based Provisioning" for more information.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates Up To Release 9.0.4.3
- Documentation-Specific Updates in Release 9.0.4.12

Documentation-Specific Updates Up To Release 9.0.4.3

The following are documentation-specific updates up to release 9.0.4.3:

- Instructions for installing the connector on Oracle Identity Manager Release 9.1.0 or Later have been added. See the "Installing the Connector on Oracle Identity Manager Release 9.1.0.x and Release 11.1.1" section for more information.
- Microsoft Windows 2000 Server is no longer a supported host for the target system. All occurrences of "Microsoft Windows 2000" have been removed from this guide.'
- In the "Multilanguage Support" section, Arabic has been added to the list of languages that the connector supports.
- In the "Step 1: Verifying Deployment Requirements" section, changes have been made in the "Target system and target system host platforms" row.
- From this release onward:

  The minimum certified release of Oracle Identity Manager is release 9.1.0.1.

  The minimum certified release of JDK is release 1.4.2.

  See "Step 1: Verifying Deployment Requirements" section for the complete listing of certified components.

Documentation-Specific Updates in Release 9.0.4.12

The testing utility is not supported in this release. The chapter that explained the procedure to use this utility has been removed.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for RSA Authentication Manager is used to integrate Oracle Identity Manager with RSA Authentication Manager.

This chapter contains the following sections:

- Certified Components
- Certified Languages
- Reconciliation Module
- Provisioning Module
- Supported Functionality
- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector

> **Note:** In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.
>
> At some places in this guide, RSA Authentication Manager has been referred to as the *target system*.

1.1 Certified Components

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

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.0.1 through release 9.0.3.2 ■ Oracle Identity Manager release 9.1.0.1 **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1) **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1). The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at `http://www.oracle.com/technetwork/documentation/oim1014-097544.html`
Target system and target system host platforms	The target system can be any one of the following: ■ RSA ACE/Server 5.2 on Windows Server 2003, Solaris 8, Solaris 9, Solaris 10 ■ RSA Authentication Manager 6.0 on Windows Server 2003 ■ RSA Authentication Manager 6.1 on Windows Server 2003 ■ RSA Authentication Manager 6.1.2 on Solaris 9, Solaris 10
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.2, or a later release in the 1.4.2 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.
Other systems	RSA SecurID software token application **See Also:** The "Installing Software Tokens" section for more information about the RSA SecurID software token

1.2 Certified Languages

The connector supports the following languages:

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

- Portuguese (Brazilian)
- Spanish

> **See Also:** For information about supported special characters
>
> - For Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*, see *Oracle Identity Manager Globalization Guide*.
> - For Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

1.3 Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

> **See Also:** One of the following guides for conceptual information about reconciliation configurations:
>
> - For Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*, see *Oracle Identity Manager Connector Concepts Guide*.
> - For Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

This section discusses the following topics:

- Reconciled Resource Object Fields
- Reconciled Xellerate User Fields
- Reconciliation of Multivalue Attribute Groups

1.3.1 Reconciled Resource Object Fields

The following target system fields are reconciled:

- Default Login
- First Name
- Last Name
- Temporary User
- Start Date
- Start Time
- End Date
- End Time
- Group Name
- Group Login
- Key Value
- Data Value
- Token Serial Number

- Type of Token

1.3.2 Reconciled Xellerate User Fields

The following target system fields are reconciled only if trusted source reconciliation is implemented:

- User ID
- First Name
- Last Name
- Employee Type
- User Type
- Organization

1.3.3 Reconciliation of Multivalue Attribute Groups

The following are features related to the reconciliation of multivalue attribute groups:

- Group names that include the names of sites are entered in the `group_name@domain_name` format. In Oracle Identity Manager 9.0.3, you can choose not to include the domain name while creating or updating the name of a group. Similarly, regardless of whether or not the name of a group in the target system includes a domain name, it is reconciled in Oracle Identity Manager.

  > **Note:** The term "domain name" in the Oracle Identity Manager context is the same as "site name" in RSA Authentication Manager.

- When a user is deleted from a group in ACE, the group is also deleted from the user's ACE process child table.

1.4 Provisioning Module

Provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. You use the Administrative and User Console to perform provisioning operations.

> **See Also:** One of the following guides for conceptual information about provisioning:
>
> - For Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*, see *Oracle Identity Manager Connector Concepts Guide*.
> - For Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*.

For this target system, provisioning is divided into the following types:

- RSA Authentication Manager User Provisioning
- RSA Authentication Manager Token Provisioning

1.4.1 RSA Authentication Manager User Provisioning

In this provisioning type, you can specify values for the following fields:

- Default Login
- First Name
- Last Name
- Temporary User
- Start Date
- Start Time
- End Date
- End Time
- Group Login
- Group Name
- Key Value
- Data Value

1.4.2 RSA Authentication Manager Token Provisioning

In this provisioning type, you can specify values for the following fields:

- Token Serial Number
- PIN
- Current Token Code
- Lifetime (hours)
- Number of Digits
- Type of Token
- Copy Protection Flag
- Password
- Password Usage and Interpretation Method
- Software Token File Name
- Encryption Key Type
- Type of Algorithm

1.5 Supported Functionality

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

Function	Description
Create User	Creates a user
Update User	Updates the identity attributes of a provisioned user

Function	Description
Delete User	Deletes a user This function would not run if the user to be deleted is an administrator.
Enable Token	Enables a disabled token
Disable Token	Disables an existing token
Assign SecurID Tokens to Users	Assigns a token to a user While assigning a software token to the user, the **Type of Algorithm** field must be filled in the process form. ■ If `SID` is selected in the Type of Algorithm field, then values must be specified for the following fields in the process form: - Software Token File Name: This is the name of the RSA SecurID software token file in which user and token information is saved. You must enter the file name with the full directory path and ensure that the extension is `.sdtid`. - Encryption Key Type - Copy Protection Flag - Password Usage and Interpretation Method - Password - Encryption Key Type - Password Usage and Interpretation Method - Password **Note:** If these combinations do not matter, then you can accept the default options. ■ If `AES` is specified in the Type of Algorithm field, then: You must enter a value in the Software Token File Name field of the process form. This is the name of the RSA SecurID software token file in which user and token information is saved. You must enter the file name with the full directory path and ensure that the extension is `.sdtid`. The Password field is optional. The following fields can be ignored: - Encryption Key Type - Copy Protection Flag - Password Usage and Interpretation Method
Revoke SecurID Tokens from Users	Revokes a token from a user

Function	Description
Assign Users to RSA Authentication Manager Groups	Assigns a user to a group You must ensure that the following prerequisites are met before you use this function: ■ Valid groups exist in RSA Authentication Manager. ■ The required lookup codes (corresponding to valid group names) are added in the `UD_Lookup.ACE_Group` lookup definition. For example, for a group called `Managers` defined in ACE DB, the following entry must be added as the lookup code: **Code Key:** `Managers` **Decode:** `Managers` **Lang:** `en` **Country:** `US`
Remove Users from RSA Authentication Manager Groups	Removes a user from a group You must ensure that the following prerequisites are met before you use this function: ■ Valid groups exist in ACE DB. ■ This function is run only after the Assign Users to RSA Authentication Manager Groups function has been run.
Set Token PIN	Updates the configuration of a token according to a change in the PIN attribute
Set PIN to Next Token Code Mode	Sets the PIN to the next token code mode in RSA Authentication Manager
Track Lost Tokens	Updates the configuration of a token according to a change in the Track Lost attribute
Test Login	Verifies the login for a new user to whom a token has been assigned You must ensure that the following prerequisites are met before you use this function: ■ An agent host is defined in the RSA Authentication Manager database. ■ The user for whom the Test Login function is to be implemented is enabled on this agent host. After this is done, the RSA Authentication Manager is restarted (Broker as well as Authentication Server). For software token types, you must enter the passcode, instead of the token code, in the Current Token Code field in the process form. The passcode can be viewed by using the software token application, which is installed on the Oracle Identity Manager server. **See Also**: The "Installing Software Tokens" section for more information
Add key-data pairs to user extension data	Adds a key-data pair to user extension data Before you use this function, you must ensure that the following prerequisite is met: User must not have user extension data with the same key before provisioning to the target system.

Function	Description
Update key-data pairs in user extension data	Update a key-data pair in user extension data Before you use this function, you must ensure that the following prerequisites are met: ■ User must have user extension data with the same key value before provision to the target system. ■ You must not change the key value. Only the data value needs to be change before provisioning.
Delete key-data pairs from user extension data	Delete a key-data pair user extension data Before you use this function, you must ensure that the following prerequisite is met: User must have user extension data with the same key value before provisioning to the target system.

See Also: Appendix A, "Attribute Mappings Between Oracle Identity Manager and RSA Authentication Manager"

1.6 Files and Directories That Comprise the Connector

The files and directories that comprise this connector are listed and described in Table 1–2.

Table 1–2 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
Files in the `DataSets` directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
`lib/xliACE.jar`	This JAR file contains the class files required for provisioning. During connector installation, this file is copied to the following location: ■ For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
`lib/xliACERecon.jar`	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location: ■ For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
`remotePackage/config/xl.policy`	This file contains the security configuration that is required for the RMI server codebase for running calls on RSA Authentication Manager for reconciliation.
`remotePackage/lib/ACE52/ACEUser.dll`	This file contains the shared library that is required to support provisioning in RSA ACE Server 5.2.
`remotePackage/lib/ACE52Sol/libACEUser.so`	This file contains the shared library that is required to support provisioning in RSA Authentication Manager.

Table 1–2 (Cont.) Files and Directories On the Installation Media

File in the Installation Media Directory	Description
`remotePackage/lib/AuthMgr60/ACEUser.dll`	This file contains the shared library that is required to support provisioning in RSA Authentication Manager 6.0.
`remotePackage/lib/AuthMgr61/ACEUser.dll`	This file contains the shared library that is required to support provisioning in RSA Authentication Manager 6.1, on Microsoft Windows.
`remotePackage/lib/xliACERemote.jar`	This file contains the Java classes that are required for provisioning to RSA Authentication Manager and reconciliation from RSA Authentication Manager to Oracle Identity Manager.
`remotePackage/scripts/AuthMgrImportXLCert.bat`	This file contains the script for importing the required security certificate into the remote manager keystore (`.xlkeystore`).
`remotePackage/scripts/AuthMgrImportXLCert.sh`	This file contains the script for importing the required security certificate into the remote manager keystore (`.xlkeystore`) on Solaris.
`remotePackage/tests/config/xl.policy`	This file contains the security configuration required for the RMI server codebase to run test calls on RSA Authentication Manager.
`remotePackage/tests/lib/xliACETestServer.jar`	This file contains the Java classes that are required to run the RMI server for running test calls on RSA Authentication Manager.
`remotePackage/tests/scripts/runTestServer.bat`	This file contains the script that is required to run the RMI server for running test calls on RSA Authentication Manager.
`remotePackage/tests/scripts/runTestServer.sh`	This file contains the script that is required to run the RMI server for running test calls on RSA Authentication Manager, on Solaris.
Files in the `resources` directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through release 9.0.3.2 and release 9.1.0.*x*: *OIM_HOME* / xellerate / connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
`scripts/AuthMgrImportRMCert.bat`	This file contains the script for importing the required security certificate in the Oracle Identity Manager server keystore (`.xlkeystore`).
`scripts/AuthMgrImportRMCert.sh`	This file contains the script for importing the required security certificate in the Oracle Identity Manager server keystore (`.xlkeystore`) on Solaris.
`tests/config/config.properties`	This file contains the properties required by the RMI client for running test calls from the Oracle Identity Manager server.
`tests/lib/xliACETestClient.jar`	This file contains the Java classes required to run the RMI client for running test calls from the Oracle Identity Manager server.

Table 1–2 (Cont.) Files and Directories On the Installation Media

File in the Installation Media Directory	Description
`tests/scripts/runTestClient.bat`	This file contains the script required to run the RMI client for running test calls from the Oracle Identity Manager Server, for Microsoft Windows.
`tests/scripts/runTestClient.sh`	This file contains the script required to run the RMI client for running test calls from the Oracle Identity Manager Server, for Solaris.
`xml/RSAAuthManagerResourceObject.xml`	This file contains definitions for the following ACE User and ACE Token components of the connector: ■ IT Resource definition ■ IT Resource ■ Process forms ■ Process task and rule-generator adapters (along with their mappings) ■ Resource objects ■ Provisioning process ■ Pre-populate rules that are used with this connector ■ Reconciliation scheduled tasks
`xml/RSAAuthManagerXLResourceObject.xml`	This file contains configuration parameters for the Xellerate User. You must import this file only if you plan to use the connector in trusted source reconciliation mode.

Note: The files in the `tests` directory are used only to run tests on the connector.

The "Copying Connector Files" section provides instructions to copy these files into the required directories.

1.7 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.0.1 through release 9.0.3.2 and release 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1, then skip this section.

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

1. Extract the contents of the `xliACE.jar` file. This file is in the following directory on the installation media:

   ```
   Security Applications/RSA Authentication Manager
   ```

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xliACE.jar` file.

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

2 Deploying the Connector

The following sections describe procedures involved in deploying the connector:

- Installing the Connector on Oracle Identity Manager Release 9.1.0.x and Release 11.1.1
- Installing the Connector on Oracle Identity Manager Release 9.0.1 Through Release 9.0.3.2
- Configuring the Oracle Identity Manager Server
- Configuring the Target System
- Configuring the Connector in Remote Mode
- Providing Minimum Access Rights to RSA Authentication User in Remote Mode
- Installing Software Tokens

2.1 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x* and Release 11.1.1

Installing the connector on Oracle Identity Manager release 9.1.0.*x* and release 11.1.1 involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.1.1 Running the Connector Installer

Note:

Perform the procedure described in this section only if you are installing the connector on Oracle Identity Manager release 11.1.1.

In this guide, the term **Connector Installer** has been used to refer to the Connector Installer feature of the Oracle Identity Manager Administrative and User Console.

To run the Connector Installer:

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

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

- For Oracle Identity Manager release 9.1.0.*x*:
  OIM_HOME/xellerate/ConnectorDefaultDirectory
- For Oracle Identity Manager release 11.1.1:
  OIM_HOME/server/ConnectorDefaultDirectory

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

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

     Oracle Identity Manager Administrative and User Console Guide

   - For Oracle Identity Manager release 11.1.1:

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

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

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

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

   - For Oracle Identity Manager release 11.1.1:

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

4. From the Connector List list, select **RSA Authentication Manager *RELEASE_NUMBER*.** This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

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

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

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

   c. From the Connector List list, select **RSA Authentication Manager *RELEASE_NUMBER*.**

5. Click **Load**.

6. 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). If you want to import the target system as a trusted source for reconciliation, then see "Configuring Trusted Source Reconciliation".

   c. Compilation of adapters.

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed.

Depending on the reason for the failure, make the required correction and then perform one of the following steps:

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

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

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

   > **Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See "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

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

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

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer.

Installing the Connector in an Oracle Identity Manager Cluster

While installing the connector in an Oracle Identity Manager cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Section 2.2.1, "Copying Connector Files" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.1.2 Configuring the IT Resource

To specify values for the parameters of the ACE Remote Manager and ACE Server Remote IT resources:

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management**, and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter the name of the IT resource 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. The "Configuring the IT Resource" section describes the parameters of both IT resources.
8. To save the values, click **Update**.

2.2 Installing the Connector on Oracle Identity Manager Release 9.0.1 Through Release 9.0.3.2

Note: Perform the procedure described in this section only if you are installing the connector on any Oracle Identity Manager release from 9.0.1 through 9.0.3.2.

Installing the connector on an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 involves the following procedures:

- Section 2.2.1, "Copying Connector Files"
- Section 2.2.2, "Importing the Connector XML Files"
- Section 2.2.3, "Compiling Adapters"

2.2.1 Copying Connector Files

The connector files to be copied and the directories to which you must copy them are given in the following table.

See Also: "Files and Directories That Comprise the Connector" on page 1-8 for more information about these files

File in the Installation Media Directory	Destination Directory
Directories and files in the `remotePackage` directory	- For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *OIM_HOME*/xellerate/XLIntegrations/AuthManager/remotePackage - For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/XLIntegrations/AuthManager/remotePackage **Note:** You do not need to copy this directory if you already performed the procedure described in the "Setting Up the Remote Manager" section on page 2-20.
Directories and files in the `scripts` directory	- For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *OIM_HOME*/xellerate/XLIntegrations/AuthManager/scripts - For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/XLIntegrations/AuthManager/scripts
Directories and files in the `tests` directory	- For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *OIM_HOME*/xellerate/XLIntegrations/AuthManager/tests - For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/XLIntegrations/AuthManager/tests
Files in the `xml` directory	*OIM_HOME*/xellerate/XLIntegrations/AuthManager/xml - For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*: *OIM_HOME*/xellerate/XLIntegrations/AuthManager/xml - For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/XLIntegrations/AuthManager/xml

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

2.2.2 Importing the Connector XML Files

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-8, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML files into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `RSAAuthManagerResourceObject.xml` file, which is in the *`OIM_HOME`*`/xellerate/XLIntegrations/AuthManager/xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the `ACE Remote Manager` IT resource is displayed.
8. Specify values for the parameters of the `ACE Remote Manager` IT resource. Refer to the "Parameters of the ACE Remote Manager IT Resource" section for information about the values to be specified.
9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `Remote Manager` IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Provide IT Resource Instance Data page for the `ACE Server Remote` IT resource is displayed.

    See Also: If you want to define another IT resource, then refer to *Oracle Identity Manager Administrative and User Console Guide* for instructions.

11. Specify values for the parameters of the `ACE Server Remote` IT resource. Refer to the "Parameters of the ACE Server Remote IT Resource" section for information about the values to be specified.
12. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the `ACE Server` IT resource type is displayed.
13. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.
14. Click **View Selections**.

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

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

After you import the connector XML files, proceed to the next chapter.

2.2.3 Compiling Adapters

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

- `ACE ASSIGN TO GROUP`
- `ACE DELETE USER`

- `ACE CREATE USER`
- `SetRSAUserAttribute`
- `ACE PrePop DefLogin`
- `ACE PrePop FirstName`
- `ACE PrePop GrpLogin`
- `ACE PrePop LastName`
- `ACE ASSIGN TOKEN`
- `ACE REMOVE TOKEN`
- `ACE DISABLE TOKEN`
- `ACE SET PIN`
- `ACE SET PIN TO NTC`
- `ACE TRACK LOST TOKEN`
- `ACE ENABLE TOKEN`
- `ACE TEST LOGIN`
- `ACE ADD USER EXTENSION DATA TO USER`
- `ACE UPDATE USER EXTENSION DATA FOR USER`
- `ACE DEL USER EXTENSION DATA TO USER`
- `Set Temporary User`

You must compile these adapters before they can be used in provisioning operations.

To compile adapters by using the Adapter Manager form:

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

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

   Note: Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an `OK` compilation status.

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. In an Oracle Identity Manager cluster, copy the compiled adapters from the *`OIM_HOME`*`/xellerate/Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

If you want to compile one adapter at a time, then use the Adapter Factory form.

See Also: *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

To view detailed information about an adapter:

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

2.3 Defining IT Resources

The following sections provide information about the IT resource parameters:

- Section 2.3.1, "Parameters of the ACE Remote Manager IT Resource"
- Section 2.3.2, "Parameters of the ACE Server Remote IT Resource"

2.3.1 Parameters of the ACE Remote Manager IT Resource

You must specify values for the `ACE Remote Manager` IT resource parameters listed in the following table:

Parameter	Description
`service name`	Remote manager service name `RManager`
`url`	Remote manager URL For example: `rmi://10.1.1.114:12346`

2.3.2 Parameters of the ACE Server Remote IT Resource

You must specify values for the `ACE Server Remote` IT resource parameters listed in the following table:

Parameter	Description
`ACEAdminMode`	Admin mode through which the connector connects to RSA Authentication Manager for provisioning and reconciliation The value can be `Host` or `Remote`. Note: If the value is Remote, then remote manager service will login to RSA Authentication Manager using the user credentials ACEAdminPassCode and `ACEAdminUserId`. If `ACEAdminMode` is in Host mode and if Remote Manager is started as Windows service, then that service has to be run under OS user who has installed RSA Authentication Manager. If `ACEAdminMode` is in Host mode, then Remote Manager starts with OS user who has installed RSA Authentication Manager.
`ACEAdminPassCode`	Admin passcode, which is required only when the admin mode is `Remote` The value is encrypted after the changes to the IT resource are saved. Sample value: `123456` See the "Configuring the Connector in Remote Mode by Using a Dynamic Passcode" section for information about the values you can specify for this parameter.
`ACEAdminUserId`	Admin user ID, which is required when the admin mode is either `Remote` or `Host`.
`Target Locale: Country`	Country code Default value: `US` Note: You must specify the value in uppercase.

Parameter	Description
`Target Locale: Language`	Language code You can select one of the following: ■ English: `en` ■ Japanese: `jp` ■ French: `fr` Note: You must specify the value in lowercase.

2.4 Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves performing the following procedures:

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

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging
- Configuring Trusted Source Reconciliation
- Configuring Oracle Identity Manager Release 11.1.1 for Request-Based Provisioning

2.4.1 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.

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

While performing the instructions described in the "Copying Connector Files" section on page 2-4, the resource bundles are copied from the resources directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory on an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x* and into the Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, perform one of the following steps:
   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/bin directory.

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

For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

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

For Oracle Identity Manager release 11.1.1:

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

2. Enter one of the following commands:

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

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

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

- For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

  On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`

  On UNIX: `PurgeCache.sh ConnectorResourceBundle`

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

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

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

  ```
  t3://OIM_HOST_NAME:OIM_PORT_NUMBER
  ```

  In this format:

- Replace `OIM_HOST_NAME` with the host name or IP address of the Oracle Identity Manager host computer.
- Replace `OIM_PORT_NUMBER` with the port on which Oracle Identity Manager is listening.

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

2.4.3 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform the procedure described in one of the following sections:

- Enabling Logging on an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or Release 9.1.0.x
- Enabling Logging on Oracle Identity Manager Release 11.1.1

Then, perform the following procedure:

- Enabling Logging for the Remote Manager

2.4.3.1 Enabling Logging on an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or Release 9.1.0.*x*

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

> **Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

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

- `ALL`

  This level enables logging for all events.

- `DEBUG`

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

- `INFO`

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

- `WARN`

  This level enables logging of information about potentially harmful situations.

- `ERROR`

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

- `FATAL`

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

- `OFF`

  This level disables logging for all events.

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

- **IBM WebSphere Application Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.RSA_ACE=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.RSA_ACE=INFO
     ```

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

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

- **JBoss Application Server**

  To enable logging:

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

     ```
     <category name="XELLERATE">
        <priority value="log_level"/>
     </category>

     <category name="XL_INTG.RSA_ACE">
        <priority value="log_level"/>
     </category>
     ```

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

     ```
     <category name="XELLERATE">
        <priority value="INFO"/>
     </category>

     <category name="XL_INTG.RSA_ACE">
        <priority value="INFO"/>
     </category>
     ```

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

  JBoss_home/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

   ```
   log4j.logger.XELLERATE=log_level
   log4j.logger.XL_INTG.RSA_ACE=log_level
   ```

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

   For example:

   ```
   log4j.logger.XELLERATE=INFO
   log4j.logger.XL_INTG.RSA_ACE=INFO
   ```

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

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

- **Oracle WebLogic Server**

  To enable logging:

  1. Add the following lines in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.RSA_ACE=log_level
     ```

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

     For example:

     ```
     log4j.logger.XELLERATE=INFO
     log4j.logger.XL_INTG.RSA_ACE=INFO
     ```

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

  ```
  WebLogic_home/user_projects/domains/domain_name/server_name/server_name.log
  ```

2.4.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

> **Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.1 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 log levels are mapped to ODL message type and level combinations as shown in Table 2–1.

Table 2–1 Log Levels and ODL Message Type:Level Combinations

Log 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_SERVER* 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='rsa-ace-handler' 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="XL_INTG.RSA_ACE" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="rsa-ace-handler"/>
     <handler name="console-handler"/>
   </logger>
```

b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–1 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='rsa-ace-handler' 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="XL_INTG.RSA_ACE" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="rsa-ace-handler"/>
     <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.

2.4.3.3 Enabling Logging for the Remote Manager

To enable logging for the Remote Manager:

1. Add the following lines in the *RemoteManager_home*/`xlremote/config/log.properties` file:

```
log4j.rootLogger=WARN,stdout,logfile
log4j.appender.logfile.File=log_file_path_and_name
log4j.logger.XELLERATE=log_level
log4j.logger.XL_INTG.RSA_ACE=log_level
```

2. In these lines, replace *log_file_path_and_name* with the full path and name of the log file and *log_level* with the log level that you want to set.

   For example:

   ```
   log4j.rootLogger=WARN,stdout,logfile
   log4j.appender.logfile.File=c:/rm_rsa_ace_connector.log
   log4j.logger.XELLERATE=INFO
   log4j.logger.XL_INTG.RSA_ACE=INFO
   ```

After you enable logging, log information is written to the file that you specify as the value of the `log4j.appender.logfile.File` attribute.

2.4.4 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

> **Note:** You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, `RSAAuthManagerXLResourceObject.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.

   > **Note:** Only one target system can be designated as a trusted source. If you import the `RSAAuthManagerXLResourceObject.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Set the `IsTrusted` scheduled task attribute to `True`. You specify a value for this attribute while configuring the user reconciliation scheduled task, which is described later in this guide.

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation pane.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.

4. Locate and open the RSAAuthManagerXLResourceObject.xml file located in the following directory:

   - For an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*:

     OIM_HOME/xellerate/XLIntegrations/AuthManager/xml

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/XLIntegrations/AuthManager/xml

   Details of this XML file are shown on the File Preview page.

5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

After you import the XML file for trusted source reconciliation, you must set the value of the `IsTrusted` reconciliation scheduled task attribute to `True`. This procedure is described in the "Configuring the Reconciliation Scheduled Tasks" section.

2.4.5 Configuring Oracle Identity Manager Release 11.1.1 for Request-Based Provisioning

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

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

The following are features of request-based provisioning:

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

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

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

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

- Section 2.4.5.1, "Copying Predefined Request Datasets"
- Section 2.4.5.2, "Importing Request Datasets into MDS"
- Section 2.4.5.3, "Enabling the Auto Save Form Feature"
- Section 2.4.5.4, "Running the PurgeCache Utility"

2.4.5.1 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 predefined request dataset available in the DataSets directory on the installation media:

- ModifyAuth Manager User.xml
- ModifyAuth Manager Token.xml
- ProvisionAuth Manager User.xml
- ProvisionResourceAuth Manager Token.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\AuthMgr

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

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

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

2.4.5.2 Importing Request Datasets into MDS

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

To import a request dataset definition into MDS:

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

> **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.4.5.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\AuthMgr directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

2. In a command window, change to the *OIM_HOME*\server\bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

4. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`
   - `Please enter your password [weblogic]`

     Enter the password used to log in to the WebLogic server.
   - `Please enter your server URL [t3://localhost:7001]`

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

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

     In this format, replace:

     – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

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

   The request dataset is imported into MDS.

2.4.5.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

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

2.4.5.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.4.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.5 Configuring the Target System

Configuring the target system involves the following steps:

- Setting Up the Remote Manager

- Configuring Strong Authentication Between Oracle Identity Manager and the Remote Manager
- Configuring SSL Client (Oracle Identity Manager Server) Authentication

2.5.1 Setting Up the Remote Manager

To set up the remote manager on the RSA Authentication Manager server:

> **Note:** For Solaris, you must create an ACE administrator as a preinstallation requirement for RSA Authentication Manager. This administrator is the file owner of the RSA Authentication Manager installation. Use this ACE administrator account to install the remote manager.

1. Create the `AuthManager` directory on the RSA Authentication Manager server.
2. From the installation media directory, copy the `remotePackage` directory into the `AuthManager` directory.

   For Solaris

   Log in to the Solaris server by using the user credentials of the RSA Authentication Manager File Owner that was created as a preinstallation requirement for RSA Authentication Manager. Then, create the directory into which you copy the `remotePackage` directory.

   > **Note:** If you copy files from Microsoft Windows to Solaris, all data transfer from the FTP client must be performed in binary mode. In addition, after copying files to the Solaris server, you must check the files for the `^M` character pattern.
   >
   > You must also perform required operations, such as `dos2unix.` As described earlier, copy all the files while using the ACE administrator credentials.

3. To update the class files, copy the `authmgr_home/lib/xliACERemote.jar` file from the installation media directory to the *`xl_remote`*`/xlremote/JavaTasks` directory.

   > **Note:** From this point onward in the guide, the full path of the `remotePackage` directory on the RSA Authentication Manager server is referred to as *`authmgr_home`*.

4. Update the library files as follows:

   - **On Microsoft Windows:**

     Use a text editor to open the following file:

     `xl_remote``/xlremote/remotemanager.bat`

     In this file, depending on the version of Authentication Manager that you are using, set one of the following as the first line of the file:

     For ACE 5.2:

```
set PATH=authmgr_home/lib/ACE52;%PATH%
```

For RSA Authentication Manager 6.0:

```
set PATH=authmgr_home/lib/AuthMgr60;%PATH%
```

For RSA Authentication Manager 6.1:

```
set PATH=authmgr_home/lib/AuthMgr61;%PATH%
```

- **For RSA ACE 5.2 on Solaris 8, 9, 10:**

  Set the `LD_LIBRARY_PATH` environment variable as follows:

  ```
  LD_LIBRARY_PATH=$ACE_INSTALL/prog:$AUTHMGR_HOME/lib/ACE52Sol
  export LD_LIBRARY_PATH
  ```

- **For RSA ACE 6.1.2 on Solaris 9, 10:**

  Set the `LD_LIBRARY_PATH` environment variable as follows:

  ```
  LD_LIBRARY_PATH=$ACE_INSTALL/prog:$AUTHMGR_HOME/lib/ACE612Sol
  export LD_LIBRARY_PATH
  ```

2.5.2 Configuring Strong Authentication Between Oracle Identity Manager and the Remote Manager

To configure strong authentication between Oracle Identity Manager and the remote manager, you must import the required certificate from the remote manager keystore to the Oracle Identity Manager server keystore as follows:

1. From the Oracle Identity Manager server, copy the *OIM_HOME*/xellerate/config/xlserver.cert file to the *AuthManager_home*/scripts/config directory on the RSA Authentication Manager server.

2. Use a text editor to open the *authmgr_home*/scripts/AuthMgrImportXLCert.bat file.

   In this file, set the following parameters:

   ```
   set JAVA_HOME=jdk_home
   set XL_REMOTE=xl_remote
   ```

   For Solaris, set the following parameters in the *authmgr_home*/scripts/AuthMgrImportXLCert.sh file:

   ```
   XL_REMOTE=xl_remote
   export XL_REMOTE
   JAVA_HOME=jdk_home
   export JAVA_HOME
   ```

3. Run the AuthMgrImportXLCert.bat file.

   For Solaris, run the AuthMgrImportXLCert.sh file.

2.5.3 Configuring SSL Client (Oracle Identity Manager Server) Authentication

To configure SSL client (Oracle Identity Manager server) authentication:

1. Open the *xl_remote*/xlremote/config/xlconfig.xml file.

2. In the <RMSecurity> section of this file, change the value of the <ClientAuth> element to true.

The following is a code block from the `xlconfig.xml` file:

```
<RMSecurity>
  <RMIOverSSL>true</RMIOverSSL>
  <SSLPort>12345</SSLPort>
  <SSLContextAlgorithm>TLS</SSLContextAlgorithm>
  <KeyManagerFactory>SunX509</KeyManagerFactory>
  <BindingPort>12346</BindingPort>
  <ServiceName>RManager</ServiceName>
  <LoggerConfigFilePath>log.conf</LoggerConfigFilePath>
  <ClientAuth>true</ClientAuth>
</RMSecurity>
```

Multiple Oracle Identity Manager Servers Communicating with a Single Remote Manager

If a setup involves more than one Oracle Identity Manager server communicating with a single remote manager, then you must address the considerations described in this section.

The `OIM_HOME/xellerate/config/xlserver.cert` certificate for any Oracle Identity Manager installation would have the same `dname` value. If you import this certificate from one Oracle Identity Manager installation into the target system remote manager keystore, then you cannot directly use the same certificate from another installation for the same purpose and in the same manner.

Therefore, if one Oracle Identity Manager installation is already configured with a particular remote manager and the same is needed for another Oracle Identity Manager installation, then you must first create a certificate with a different DN for the second installation before you can use this new certificate with the remote manager.

Enter the following commands in the specified order.

1. Generate a new key pair by entering the following command:

   ```
   jdk_home/jre/bin/keytool -genkey -alias xell2 -keyalg DSA -keysize 1024 -dname
   "CN=Customer1, OU=Customer, O=Customer, L=City, ST=NY, C=US" -validity 3650
   -keypass xellerate -keystore OIM_HOME/xellerate/config/.xlkeystore -storepass
   xellerate -storetype jks -provider sun.security.provider.Sun
   ```

   When you run this command, ensure that the `dname` value specified in the preceding command, is not the same as the default value of `dname,` for the existing certificates in the Oracle Identity Manager keystore:

   ```
   OIM_HOME/xellerate/config/.xlkeystore
   ```

   The default value is as follows:

   ```
   CN=Customer, OU=Customer, O=Customer, L=City, ST=NY, C=US
   ```

2. Create a certificate request by entering the following command:

   ```
   jdk_home/jre/bin/keytool -certreq -alias xell2 -file
   OIM_HOME/xellerate/config/xell1.csr -keypass xellerate -keystore
   OIM_HOME\/ellerate/config/.xlkeystore -storepass xellerate -storetype jks
   -provider sun.security.provider.Sun
   ```

3. Export the certificate to a file by entering the following command:

   ```
   jdk_home/jre/bin/keytool -export -alias xell2 -file
   OIM_HOME/xellerate/config/xlserver1.cert -keypass xellerate -keystore
   OIM_HOME/xellerate/config/.xlkeystore -storepass xellerate -storetype jks
   ```

```
-provider sun.security.provider.Sun
```

This command creates the following security certificate:

```
OIM_HOME/xellerate/config/xlserver1.cert
```

This is the certificate that you must use for configuration purposes.

4. Import the certificate into the remote manager keystore by entering the following command:

```
jdk_home/jre/bin/keytool -import -trustcacerts -alias xel2trusted -noprompt
-keystore OIM_HOME/xellerate/config/.xlkeystore -file
OIM_HOME/xellerate/config/xlserver1.cert -storepass xellerate
```

For configuring strong authentication between another Oracle Identity Manager Server installation and the remote manager, use the *OIM_HOME*/xellerate/config/xlserver1.cert file instead of the xlserver.cert file.

2.5.4 Configuring Strong Authentication Between the Remote Manager and the Oracle Identity Manager Server

To configure Oracle Identity Manager to trust the Remote Manager:

1. On the computer hosting Oracle Identity Manager, export the certificate by running the following command:

```
keytool -export -keystore KEYSTORE_FILE -storepass KEYSTORE_PASSWORD -alias
ALIAS -file CERT_FILE_NAME
```

In this command:

- *KEYSTORE_FILE* is the complete path and name of the keystore.
- *KEYSTORE_PASSWORD* is the password of the keystore.
- *ALIAS* is the alias of the certificate to be exported.
- *CERT_FILE_NAME* is the file name containing the exported certificate

The following is a sample command:

```
keytool -export -keystore
D:\March11g\Middleware\user_projects\domains\MARCHWIN\config\fmwconfig\default-
keystore.jks -storepass MyPa55word -alias xell -file oim.cer
```

2. Copy the exported certificate to any directory on the target system.

3. To import the certificate, run the following command:

```
keytool -import -keystore KEYSTORE_FILE -storepass KEYSTORE_PASSWORD -alias
ALIAS -file CERT_FILE_NAME
```

In this command:

- *KEYSTORE_FILE* is the complete path and name of the keystore.
- *KEYSTORE_PASSWORD* is the password of the keystore.
- *ALIAS* is the alias of the certificate to be imported.
- *CERT_FILE_NAME* is the file name containing the imported certificate

The following is a sample command:

```
keytool -import -keystore
C:\Oracle\Middleware1\Oracle_IDM1\remote_manager\config\default-keystore.jks
-storepass MyPa55word -alias oimserver -file
C:\Oracle\Middleware1\OIMCert\oim.cer
```

4. Copy the *OIM_HOME*\server\config\xlserver.cert file from the Remote Manager host computer to a temporary directory on the Oracle Identity Manager host computer.
5. To import the certificate, run the following command:

   ```
   keytool -import -keystore KEYSTORE_FILE -storepass KEYSTORE_PASSWORD -alias
   ALIAS -file CERT_FILE_NAME
   ```

   In this command:

   - *KEYSTORE_FILE* is the complete path and name of the keystore.
   - *KEYSTORE_PASSWORD* is the password of the keystore.
   - *ALIAS* is the alias of the certificate to be imported.
   - *CERT_FILE_NAME* is the file name containing the imported certificate

   The following is a sample command

   ```
   keytool -import -keystore
   D:\March11g\Middleware\user_projects\domains\MARCHWIN\config\fmwconfig\default_
   keystore.jks -storepass Welcome1 -alias rmcert -file
   D:\March11g\Middleware\RMCert146\xlserver.cert
   ```

To set up the remote manager as a trusted source for Oracle Identity Manager:

1. On the RSA Authentication Manager server, copy the `xl_remote/xlremote/config/xlserver.cert` file into the following directory:

   ```
   OIM_HOME/xellerate/XLIntegrations/AuthManager/scripts/config
   ```

2. Use a text editor to open the following file:

   ```
   OIM_HOME/xellerate/XLIntegrations/AuthManager/scripts/AuthMgrImportRMCert.bat
   ```

   In this file, edit the following lines to specify the path to the JDK and Oracle Identity Manager installation directories:

   ```
   set JAVA_HOME = jdk_home
   set XELLERATE_HOME = OIM_HOME
   ```

   For Oracle Identity Manager installed on Solaris, open the following file in a text editor:

   ```
   OIM_HOME/xellerate/XLIntegrations/AuthManager/scripts/AuthMgrImportRMCert.sh
   ```

   In this file, edit the following lines to specify the path to the JDK and Oracle Identity Manager installation directories:

   ```
   JAVA_HOME = jdk_home
   export JAVA_HOME
   XELLERATE_HOME = OIM_HOME
   export XELLERATE_HOME
   ```

3. Run the `AuthMgrImportRMCert.bat` file.

For Oracle Identity Manager installed on Solaris, run the `AuthMgrImportRMCert.sh` file.

2.6 Configuring the Connector in Remote Mode

The RSA Authentication Manager connector can be configured in remote mode by using either a dynamic passcode or a static password. The following sections provide information about the procedure:

> **Note:** You specify your choice by entering a value for the ACEAdminPassCode parameter of the ACE Server Remote IT resource. The "Parameters of the ACE Server Remote IT Resource" section provides information about this IT resource.

- Configuring the Connector in Remote Mode by Using a Dynamic Passcode
- Configuring RSA Authentication Manager Connector in Remote Mode by Using a Static Password

2.6.1 Configuring the Connector in Remote Mode by Using a Dynamic Passcode

To configuring the connector in remote mode by using a dynamic passcode:

1. Create a user in ACE server. For example, remoteAdminUser in host mode.
2. From the User menu in RSA Authentication Manager, click **Edit User** and select the user created in Step 1.
3. Click **Administrative Role**.
4. In the Change Administrative Role pop-up window, select **Administrator** as user type and click **OK**.
5. From the System menu, click **Edit System Configuration**, and then click **Edit System Parameter.**
6. In the Administration Authentication Methods of the System Parameters window, select **Secure ID Software Tokens** and click **OK**.
7. Assign the token to remoteAdminUser by performing the following steps:

   a. From the token menu, select **Issue Software Tokens.**

   b. Select the appropriate algorithm. For example, SID SDTID Algorithm.

   c. In the Password Protect field, select **Static Password** and enter the password.

   d. Enter the target directory path and file name where SDTID file has to be generated and click **Next**. The file name extension should be .sdtid.

   e. In the RSA SecureID Software Token Selection Users pop-up window, select the user and click **Next**.

   f. In the Select User window, select **remoteAdminUser** and click **OK**.

   g. In the Verify RSA SecureID Software Token Issuing List window, click **Next**.

   h. In the RSA SecureID Software Token window, select **User authenticate with passcode** and click **Next**.

   i. In the Continue Issuing RSA SecureID Software Tokens pop-up window, click **Yes**.

j. In the Save Software Token pop-up window, click **Yes** and provide the path to save. If you do not want to save, click **No**.

8. Launch the SecureID Software Tokens by clicking **Start**, **All Programs**, **SecureID Software Token**.
9. From the SecureID Software Token, select **File Menu** and then click **Import Tokens**.
10. Locate the stdid file that you created in step D of step 7.
11. Enter the password that you provided in step C of step 7 and click **OK**.
12. Select the token and click **Transfer Selected Token to Hardware Drive**.
13. In the Software Token API pop-up window, click **Yes**.
14. In the Token List Box of Select Token popup window, select software token of remoteAdminUser and click **OK**. An eight digit token codes that changes every 60 seconds in RSA SecureID is displayed.
15. From the View menu, select **Advance View** in RSA SecureID.
16. From RSA SecureID, copy the current Tokencode.
17. In the user menu of RSA Authentication Manager, click **Edit User**.
18. Select **remoteAdminUser** and click **OK**.
19. In the Tokens textbox, double-click on the token assigned to the user.
20. In the Edit Token window, click **Set PIN to Next Tokencode**.
21. Enter the token code that you copied in step 16 and click **OK**.
22. Note the first four digits of the next token code as this is the PIN of RSA SecureID.
23. Enter the PIN value that you noted in RSA SecureID and click **Apply Pin**. SecureID Software Token starts generating the passcode values.
24. Copy the current **PASSCODE**.
25. Launch the RSA Authentication Manager in the Database Administrator Remote Mode by clicking **Start**, **All Programs**, **RSA Authentication Manager**.
26. In the Select Server to Administer window, click **Ok**.
27. Enter **remoteAdminUser** as user login ID.
28. Enter the passcode value that is copied in the step 24 and click **OK**. A user authentication successful message is displayed.

2.6.2 Configuring RSA Authentication Manager Connector in Remote Mode by Using a Static Password

To configuring the connector in remote mode by using a static password:

1. Create a user in ACE server. For example, remoteAdminUser in host mode.
2. From the User menu in RSA Authentication Manager, click **Edit User** and select the user created in Step 1.
3. Click **Administrative Role**.
4. In the Change Administrative Role pop-up window, select **Administrator** as user type and click **OK**.

5. From the System menu, click **Edit System Configuration**, and then click **Edit System Parameter.**
6. In the Administration Authentication Methods of the System Parameters window, select **User Password** and click **OK**.
7. In the Confirmation pop-up window, click **Yes**.
8. In the User menu, click **Edit User** and then select **remoteAdminUser**.
9. In the **Edit User** window, click **Set/Change User Password**.
10. In the Enter New User Password popup window, enter the password and click **OK**.
11. In the Enter New User Password pop-up window, click **Ok**.
12. In the Edit User window, click **Ok**.
13. Open RSA Auth Manager in the Database Administrator Remote Mode.
14. In the Select Server to Administrator window, click **Ok**.
15. In the Administrator Authentication pop-up window, enter user login and passcode that you created in step 11 and click **OK**.
16. In the Do you want the system to generate your new PIN? [y/n] dialog box, enter **n** and click **OK**.
17. Enter the new PIN between 4 to 8 digits and click on **Ok**.
18. In the Confirm PIN field, reenter the new PIN and **Ok**. A user authentication successful message is displayed.

2.7 Providing Minimum Access Rights to RSA Authentication User in Remote Mode

To provide minimum access rights to RSA authentication user:

1. Create a user in ACE server. For example, remoteAdminUser in host mode.
2. From the User menu in RSA Authentication Manager, click **Edit User** and select the user created in Step 1.
3. Click **Administrative Role**.
4. In the Change Administrative Role pop-up window, select **Administrator** as user type and click **OK**.
5. Go to Define Task List tab and click **New**.
6. In the **Task List** field, enter the name of the task.
7. From **Available Tasks** list on the left tab, select privileges, which you want to assign the user and click on right arrow to add and left arrow to remove the tasks.
8. Click **OK**.
9. Select the task that you have created from the list.
10. In the ChangeAdministrativeRole window, click **OK**.
11. In the **Edit User** window, click **Set/Change User Password**.
12. In the Enter New User Password popup window, enter the password and click **OK**.

13. In the Edit User window, click **OK**.
14. Go to System menu of ACE Server, select **Edit System Configuration**, **Edit System Parameter**.
15. Check the User Password under Administration Authentication Methods and click **OK** in the System Parameters window.

> **Note:** To enable reconciliation and provisioning, enter this static passcode as the value of the ACEAdminPassCode parameter of the ACE Server Remote IT resource.

16. In the **Confirmation** popup window, click **Yes**.
17. From the User menu click **Edit user**, and then select **remoteAdminUser**.
18. Open the RSA ACE Server in Database Administrator-Remote Mode (RSA Authentication Manager RemoteMode).
19. In the Select Server to Administer window, click **OK**.
20. Enter user Login and passcode created in Step 12 and click **OK** in the Administrator Authentication popup window. The system will prompt whether you want to generate a new PIN. Enter "`n`" and then click **OK**.
21. Enter a new PIN between four to eight digits and click **OK**.
22. Re-enter the new PIN to confirm and click **OK**.
23. Enter same pin given in previous step and click **OK**.
24. A user authentication successful message is displayed.

2.8 Installing Software Tokens

When you use this connector to run provisioning functions that are specific to software tokens, you must provide the required input parameters, such as the Token Code.

You can determine the values of these token-specific parameters only after the RSA Software Token application is installed on the Oracle Identity Manager server or on a user computer other than the Oracle Identity Manager server.

If you are using RSA SecurID software tokens, then:

1. Download RSA SecurID Token for Windows Desktops 3.0.5 from

   `http://www.rsasecurity.com/node.asp?id=1162`

2. Install the file on the Oracle Identity Manager server.
3. Copy the RSA SecurID software token file to an appropriate location on the Oracle Identity Manager server. The file to be copied is in the RSA Authentication Manager installation directory. The format of the directory path where you copy this file can be as follows:

   `target_dir_location``/Token1File/`

> **Note:** While assigning a software token to an ACE user, you must specify the name and complete location of this file (in the `db_file_location/file_name.sdtid` format) in the Software Token File Name process form field.

4. Import the `.sdtid` file into the RSA SecurID Token software application as follows:

   a. Click **Start,** and then select **Programs.**

   b. Click **RSA SecurID Software Token,** and select the subcategory **RSA SecurID Software Token.**

   The token screen is displayed.

   c. Click the **File** menu, and then select **Import Tokens.** In the dialog box that is displayed, select the `.sdtid` file mentioned in Step 3.

   For example:

   ```
   target_dir_location/Token1File/file_name.sdtid
   ```

   d. Select the token serial number, and click **Transfer Selected Tokens to Hard Drive.** The software token is imported.

   e. On the screen that is displayed, click **View** and then select **Advanced View.**

   f. On the screen that is displayed, click **View** and then select **Token View** to view the software token number.

3 Configuring the Connector

After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

> **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.

- Configuring Reconciliation
- Configuring the Connector for Multiple Installations of the Target System
- Performing Provisioning Operations
- Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

> **Note:** This chapter provides both conceptual and procedural information about customizing the connector. It is recommended that you read the conceptual information before you perform the procedures.

3.1 Configuring Reconciliation

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

- Limited Reconciliation
- Configuring the Reconciliation Scheduled Tasks
- Direct Provisioning
- Request-Based Provisioning

3.1.1 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.

For this connector, you create a filter by specifying values for the CustomReconQuery, CompareType, and GroupTokenizerForCustomReconQuery of Scheduled Task attributes while performing the procedure described in the "Configuring the Reconciliation Scheduled Tasks" section on page 3-3.

You can use the following attributes to build the query condition:

- Last Name
- First Name
- Default Login
- Permanent or Temporary
- By Token
- By User Extension
- Group

The following table lists sample query conditions:

CustomReconQuery	CompareType	Description
[none]	**Note:** You can specify any value, but it must not be an empty value because scheduler does not allow empty values attributes.	Gets all users that are available in the target system
Last Name=D	Begins With	Gets all users whose last name starts with D
Last Name=Doe	Equals To	Gets all users with Doe as their last name
Last Name=oe	Contains	Gets all users whose last name contains oe
First Name=J	Begins With	Gets all users whose first name starts with J
First Name=John	Equals To	Gets all users with John as their first name
First Name=oh	Contains	Gets all user whose first name contains oh
First Name	With Empty Value	Gets all users with empty values as first name
First Name	With Non Empty Value	Gets all users with nonempty values as first name
Default Login=j	Begins With	Gets all users whose default login starts with j
Default Login=john	Equals To	Gets all users with john as their default login
Default Login=oh	Contains	Gets all users whose default login contains oh
By Token	Lost Tokens	Gets all users with token status as Lost
By Token	All With Passwords	Gets all users who have a password
By Token	All With Expired Tokens	Gets all users with token status as Expired
By User Extension	All With Extension	Gets all users that have extension data

CustomReconQuery	CompareType	Description
`By User Extension`	`All Without Extension`	Gets all users that do not have extension data
`By User Extension=key1`	`All With Extension Keys`	Gets all users that have extension data with key as `key1`
`By User Extension=key1`	`All Without Extension Keys`	Gets all users that do not have extension data with key containing `key1`
`Permanent or Temporary`	`All Permanent`	Gets all permanent users
`Permanent or Temporary`	`All Temporary`	Gets all temporary users

If you want to reconcile users with more than one group, then you can specify multiple groups as the value of `CustomReconQuery`, for example, `CustomReconQuery=grp1,grp2,grp3`. In this example, the group names are separated by commas. You can specify the separator by specifying the value of `GroupTokenizerForCustomReconQuery`, as shown:

```
GroupTokenizerForCustomReconQuery=,
```

The following table lists sample query conditions with values for `GroupTokenizerForCustomReconQuery`:

CustomReconQuery	CompareType	GroupTokenizerFor CustomReconQuery	Description
`Group=grpParent, grpChild1` **Note:** If the group name consists of comma, you can specify any other separator, such as $.	**Note:** You can specify any value, but it must not be an empty value because scheduler does not allow empty value for attributes.	`$`	Gets all users who belong to the `grpParent,grpChild1` group
`Group=grpParent, grpChild1$ grpParent,grpChild2`	Any value	$	Gets all users who belong to the `grpParent,grpChild1` group or the `grpParent,grpChild2` group

3.1.2 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML Files" section, the scheduled tasks for lookup fields and user reconciliations are automatically created in Oracle Identity Manager. To configure the scheduled task:

1. Log in to the Administrative and User Console.
2. Do one of the following:
   a. If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.*3.2*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced.**
3. Search for and open the scheduled task as follows:

- If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.*3.2*, then:

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

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

   c. On the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**.

- If you are using Oracle Identity Manager release 11.1.1, then:

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

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

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

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

   a. If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.*3.2*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

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

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

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

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

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

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

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

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

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

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

Note:

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

- If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

Table 3–1 describes the attributes of the scheduled task.

Table 3–1 Scheduled Task Attributes

Attribute	Description	Sample Value
`IsTrusted`	Specifies whether or not reconciliation must be performed in trusted mode.	`True` or `False`
`Server`	Name of the IT resource.	`ACE Server Remote`
`Target System Recon - Resource Object name`	Name of the target system resource object corresponding to the RSA Authentication Manager User.	`Auth Manager User`
`Target System Recon - Token Resource Object name`	Name of the target system resource object corresponding to the RSA Authentication Manager User Token, which was assigned to user.	`Auth Manager Token`
`Trusted Source Recon - Resource Object name`	Name of the trusted source Resource Object.	`Xellerate User`
`IsDeleteAllowed`	Specifies whether or not the users who have been deleted in the target system should be deleted in Oracle Identity Manager.	`True` or `False`
`Start Record`	Specifies the record number from which the reconciliation for `CustomReconQuery` and `CompareType` must begin. If Scheduler Task fails after reconciling 10000 records, then you can specify the value of `StartRecord` as `10000` so that reconciliation starts from the record where it failed. You do not have to reconcile the records that have already been reconciled.	`1`
`BatchSize`	Specifies the number of records to be reconciled in a batch. **Caution:** If you specify a very high value for `BatchSize`, for example 50000, then out memory exception may occur in the Remote Manager.	`1000`

Table 3–1 (Cont.) Scheduled Task Attributes

Attribute	Description	Sample Value
FieldMapForCustomQuery	Specifies the lookup defintion name that contains the mapping between the CustomReconQuery field name and the target system equivalent number for that field name. RSA ACE Server API accepts numbers to indicate the field name in the target system.	UD_Lookup.Ace.CustomRecon.FieldMap
CompareTypeMapForCustomQuery	Specifies the lookup definition name, which contains the mapping between CompareType and its equivalent number in the target system. The CompareType is mentioned in the task scheduler. RSA ACE Server accepts numbers to indicate the operator on field to search for the mapping.	UD_Lookup.Ace.CustomRecon.CompareTypeMap
CustomReconQuery	Query condition on which reconciliation must be based. If you specify a query condition for this attribute, then the target system records are searched based on the query condition. If you want to reconcile all the target system records, then specify [None] as the value for this attribute. For more information about this parameter, refer to the "Limited Reconciliation" section on page 3-1.	[None]
CompareType	Specifies the type of comparison used in the query condition of CustomReconQuery.	Equals To
NumberOfCharactersInEachUser	Indicates the memory allocated for each user in C code. **Caution:** If you specify a very low value for NumberOfCharactersInEachUser, for example 10, then the Remote Manager's JVM may stop.	500
Organization	Specifies the name of the organization under which users are created during trusted source reconciliation.	Xellerate Users
Xellerate Type	Specifies the user type created during trusted source reconciliation. If you reconcile users in trusted mode, then you must specify a value for this attribute.	End-User
Role	Specifies the type of employment of a user in trusted source reconciliation.	Full-Time
TrustedDeleteReconObjectStatusList	Indicates the status of the list of users that need to be deleted while performing delete reconciliation in trusted mode. f you perform delete reconciliation in trusted mode, then you must specify the statuses, separated by a comma.	Enabled, Disabled, Active
TargetDeleteReconObjectStatusList	Indicates the status of the list of users that needs to be deleted during target resource reconciliation. If you delete users during target resource reconciliation, then you must specify the statuses, separated by a comma.	Enabled, Disabled, Provisioned
TrustedDeleteReconExemptedUserIDs	Specifies the list of user IDs that must be excluded from trusted delete reconciliation.	XELOPERATOR, XELSELFREG, XELSYSADM

Table 3–1 (Cont.) Scheduled Task Attributes

Attribute	Description	Sample Value
`GroupTokenizerForCustomReconQuery`	Specifies the token for the groups provided in CustomReconQuery. For more information about `GroupTokenizerForCustomReconQuery`, see "Limited Reconciliation" on page 3-1.	`$`
`IsEnableLog`	Specifies whether or not to generate a log file when performing reconciliation. The default value for the `IsEnableLog` attribute is `No`. It means that a log file is not generated. **Note:** The log file always appends the existing log file. As a result, the file size may exceed disk space. Therefore, set the value of `IsEnableLog` to `Yes` only if the user wants to debug. When the value is set to `Yes`, the `OIM_ACE_INTG.log` file is generated.	`Yes` or `No`
`LogFileLocationInRemoteManager`	Specifies the location in the Remote Manager where the log file is to be generated. The default value is `None`. It means that the log file is generated in the Remote Manager absolute path. Note: The Remote Manager absolute path is the location in which Remote Manager's `.batch` and `.sh` files are stored.	`D:\RM\log`

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

   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then click **Save Changes** to save the changes.

     Note: The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

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

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

3.2 Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of RSA Authentication Manager.

You may want to configure the connector for multiple installations of RSA Authentication Manager. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of RSA Authentication Manager.

To configure the connector for multiple installations of the target system:

> **See Also:** One of the following guides for detailed instructions on performing each step of this procedure
>
> - For Oracle Identity Manager release from 9.0.1 through 9.0.3.2 and release 9.1.0.*x*, see *Oracle Identity Manager Design Console Guide*.
> - For Oracle Identity Manager release 11.1.1, see *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*.

1. Create and configure one IT resource for each target system installation.

   The IT Resources form is in the Resource Management folder. An IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

2. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that you need to modify only the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.

   You can designate either a single or multiple installations of RSA Authentication Manager as the trusted source.

3. If required, modify the fields to be reconciled for the Xellerate User resource object.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the RSA Authentication Manager installation to which you want to provision the user.

3.3 Performing Provisioning Operations

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

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

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

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

- Provisioning triggered by policy changes

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

This section discusses the following topics:

- Section 3.3.1, "Direct Provisioning"
- Section 3.3.2, "Request-Based Provisioning"

3.3.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.
     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. From the Users menu, select **Manage**.
     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.
   - If you are using Oracle Identity Manager release 11.1.1, then:
     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then:
     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.
     b. On the Resource Profile page, click **Provision New Resource**.
   - If you are using Oracle Identity Manager release 11.1.1, then:

   a. On the user details page, click the **Resources** tab.

   b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **Auth Manager User** from the list and then click **Continue**.

6. On the Step 2: Verify Resource Selection page, click **Continue**.

7. On the Step 5: Provide Process Data for Auth Manager User Details page, enter the details of the account that you want to create on the target system and then click **Continue**.

8. On the Step 5: Provide Process Data for Auth Manager User page, search for and select a group for the user on the target system and then click **Continue**.

9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.

10. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

    - If you are using an Oracle Identity Manager release from 9.0.1 through 9.0.3.2 or release 9.1.0.*x*, then click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.

    - If you are using Oracle Identity Manager release 11.1.1, then:

      a. Close the window displaying the "Provisioning has been initiated" message.

      b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.3.2 Request-Based Provisioning

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

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

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

- Section 3.3.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.3.2.2, "Approver's Role in Request-Based Provisioning"

3.3.2.1 End User's Role in Request-Based Provisioning

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

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

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

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

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

3.3.2.2 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.

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

> **Note:** It is assumed that you have performed the procedure described in the "Configuring Oracle Identity Manager Release 11.1.1 for Request-Based Provisioning" section.

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

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **Auth Manager User** process definition.
   c. Deselect the **Auto Save Form** check box.
   d. Click the Save icon.
   e. Repeat this procedure to deselect the Auto Save Form check box for the Auth Manager Token process definition.
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 **Auth Manager User** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the Save icon.
   e. Repeat this procedure to deselect the Self Request Allowed check box for the Auth Manager Token process definition.

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

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition**.
   b. Search for and open the **Auth Manager User** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.

   e. Repeat this procedure to select the Auto Save Form check box for the Auth Manager Token process definition.

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 **Auth Manager User** resource object.

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

   d. Click the Save icon.

   e. Repeat this procedure to select the Self Request Allowed check box for the Auth Manager Token process definition.

4

Known Issues

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

- While creating a user in RSA Authentication Manager, you must not enter special characters in the Default Login field. If you enter special characters in this field, then reconciliation would not work because Oracle Identity Manager does not support special characters in the User ID field.
- The connector does not support the use of security certificates that contain non-English characters.
- The following limitation applies to the use of the Japanese, Simplified Chinese, Traditional Chinese, Korean, and French languages:

  RSA APIs do not support certain characters of the character sets of these languages. The provisioning or reconciliation operation fails if any of the field values submitted during the operation contains any one of the unsupported characters at the start of the field value. However, the operation does not fail if unsupported characters appear at any place other than the start of the field value.

  > **See Also:** For more information about the characters not supported in provisioning and reconciliation, refer to Note 421232.1 on My Oracle Support at
  >
  > `https://metalink.oracle.com`

- When creating a temporary user during provisioning, you can specify start time or end time in hours, but you can not provide the start time or end time in hours and minutes. This is because the target system API accepts these values in hours (0-23) only. If you specify the time in hours and minutes, the API will throw the error. To avoid providing the time in hours and minutes format from the UI, a lookup is provided that has values from 0 through 23 for start time and end time.
- To synchronize reconciliation of start time or end time with provisioning, if the target system start time or end time is 0-0:59, then it is rounded off to 0. The reconciliation of start time or end time is matched with the start time and end time of provisioning. If the target system start time or end time is in hour and minute, then the start time or end time value is rounded off. For example, 1 hour and 59 minutes is rounded off to 1 hour.
- RSA Authentication Manager connector cannot be configured with multiple schedulers to reconcile users from RSA Authentication Manager because RSA ACE API is not thread safe. This means that the fields of an object or class do not maintain a valid state if multiple threads are running.
- The testing utility is not supported in release 9.0.4.12.

A

Attribute Mappings Between Oracle Identity Manager and RSA Authentication Manager

The following table discusses attribute mappings between Oracle Identity Manager and RSA Authentication Manager.

> **Note:** Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:
>
> Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

Oracle Identity Manager Attribute	RSA Authentication Manager Attribute	Description
Group Login	chLogin	Login ID of this user when logged in as a member of a specific group If a group login ID is not defined, the user's regular default login is used.
Group Name	chName	Name of the group
Token Serial Number	chSerialNum	Serial number
Pin	Pin	Sets a PIN for a specified token that is assigned to a user
Set Pin	bCreatePIN	Specifies whether or not users can create their own PINs The value can be `True` or `False`.
Curent Token Code	Not mapped to an attribute in RSA Authentication Manager DB	Token code that is displayed on the token device There is no designated field in the target to store it.
Set PIN to NTC	iNextTCodeStatus	Specifies that the next autogenerated token code must be taken as the PIN for the user

Oracle Identity Manager Attribute	RSA Authentication Manager Attribute	Description
Lifetime (Hours)	datePWExpires	Date on which the password expires
Number of Digits	iNumDigits	Number of digits returned in the password generated for emergency access after a token is set to the LOST state
Set Lost	bLost	Specifies whether or not the token device is lost The default is NOT LOST.
Type of Token	iType	Token type The token can be a hardware token device or a software token authenticator.
Copy Protection Flag	bSoftID_CopyProtected	Specifies whether or not copy protection is enabled The value can be True or False.
Password	chOTPasswordsSB	Password to be provided by the RSA Authentication Manager administrator in order to access an RSA SecurID software token XML file If there is no password associated with the file, then an empty string can be passed.
Password Usage and Interpretation Method	method	Password usage and interpretation method The value can be any one of the following: ■ 0: No password ■ 1: Static password ■ 2: Default login ■ 3: Default login appended to static password
Software Token File Name	Not mapped to an attribute in RSA Authentication Manager DB	Software token file name path There is no designated field in the target to store / represent it.
Encryption Key Type	iTokenVersion	Version of the token algorithm
Type of Algorithm	iSeedSizeType	Specifies the algorithm type The value can be any one of the following: ■ SID: For 64-bit encryption ■ AES: For 128-bit encryption
First Name	chFirstName	First name
Last Name	chLastName	Last name
Default Login	chDefaultLogin	Default login ID

Index