Oracle® Identity Manager

Connector Guide for IBM Lotus Notes and Domino

Release 9.0.4

E10428-15

July 2014

Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino, Release 9.0.4

E10428-15

Primary Author: Gowri.G.R

Contributing Authors: Prakash Hulikere, Gauhar Khan, Alankrita Prakash, Deena Purushothaman

Contents

2 Deploying the Connector

3 Using the Connector

4 Extending the Functionality of the Connector

5 Testing and Troubleshooting

6 Known Issues and Limitations

Index

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with IBM Lotus Notes and Domino.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

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

For generic information about connectors, see *Oracle 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 Oracle Identity Manager Connector for IBM Lotus Notes and Domino?

This chapter provides an overview of the updates made to the software and documentation for the IBM Lotus Notes and Domino connector in release 9.0.4.14.

> **Note:** Release 9.0.4.14 of the connector comes after release 9.0.4.12. Release number 9.0.4.13 has not been used.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

The following sections discuss software updates:

- Software Updates in Release 9.0.4.1.x
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.6
- Software Updates in Release 9.0.4.7
- Software Updates in Release 9.0.4.8
- Software Updates in Release 9.0.4.11
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.14

Software Updates in Release 9.0.4.1.x

The following are software updates in release 9.0.4.1.*x*:

Resolved Issues

The following are issues resolved in release 9.0.4.1.x:

Bug Number	Issue	Resolution	Release
6699500	During a reconciliation run, the status of modified user records remained at "Event Received". In other words, the modified user records were not getting linked.	This issue has now been resolved. The status of modified user records is "Event Linked".	9.0.4.1_6739862
6813482	The Add User provisioning operation took a long time to complete.	This issue has now been resolved. The time taken to complete the Add User provisioning operation has reduced significantly.	9.0.4.1_6868231
6627965	Additional attributes added in the attributemapping_prov.properties file were not being provisioned at the time of provisioning.	This issue has now been resolved. Now, additional attributes added in the attributemapping_prov.properties file are being provisioned at the time of provisioning.	9.0.4.1+xxxx+6027293+6627965
6397485	The mail file for a Lotus user was not customizable. Therefore, if a user was provisioned with a name that already exists on the Domino server, then the existing user/mail file would be overwritten in Lotus 6.5 and exceptions were thrown in Domino 7.0.x.	This issue has now been resolved. The following fixes were made: ■ The mail file name field in the process form has been customized. (If the user leaves this field blank, then the mail file name is constructed as first name + last name). ■ A prepopulate adapter for the mail file name has been created. ■ Exception handling for Lotus 7.0 has been introduced. ■ The connector checks if the user with the same name exists and a suitable error message is returned.	9.0.4.1+6392533+6397485+6328685+6027293
6328685	During target resource reconciliation, the reconciled data was not getting linked. The status of user data remained at 'Event Received'.	This issue has now been resolved. Now, the Target reconciliation completes and events are getting linked.	9.0.4.1+6392533+6397485+6328685+6027293
6027293	Internet Users (users with user IDs in the non-DN format) were not getting reconciled.	This issue has now been resolved. Internet Users (users with user IDs in the non-DN format) are now getting reconciled.	9.0.4.1+6392533+6397485+6328685+6027293

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Support for IBM Lotus Domino Server 8.0.1
- Resolved Issues

Support for IBM Lotus Domino Server 8.0.1

IBM Lotus Domino Server 8.0.1 has been added to the list of supported target systems. The required information has been included at appropriate places in the guide.

Resolved Issues

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
6645041	The target system does not allow updates to a user's organizational unit (OU) if the user has a certifier with an associated OU. A provisioning operation that attempts this action always fails. In the earlier release of the connector, subsequent attempts to update any of the name fields failed.	You can now update any of the name fields even if the operation is preceded by a failed attempt at updating the user's OU. **Note:** The "Known Issues and Limitations" chapter lists another issue related to name fields.
6723807	A provisioning operation failed if it involved an update to a name field (for example, the Last Name field) and any other field (for example, the Comment field).	You can now update a name field and any other field. However, if you add a new field for provisioning, provisioning operations that involve updating a name field and the newly added field would fail.

Software Updates in Release 9.0.4.3

The following is a software update 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 Section 2.2.1, "Running the Connector Installer" for details.

Software Updates in Release 9.0.4.4

The following are software updates in release 9.0.4.4:

- The `UniqueID` field has been added on the process form. This field is used to uniquely identify Lotus Notes resource during reconciliation runs and provisioning operations. This field was added to address Bug 6976566, which is mentioned later in this section.

  The following changes have been made in this guide:

  - In "Reconciled Resource Object Fields" on page 1-2, the `UniqueID` field has been added to the list of fields that are reconciled.
  - In "Files and Directories on the Installation Media" on page 1-5, the `config_unid.properties` file has been added. This file holds the `UniqueID` value of the user that you create while testing provisioning operations.
  - See "Changing the Mapping of the UniqueID Field" on page 3-13 for information about mapping the `UniqueID` field to a different target system field.
  - In Appendix A, the `UniqueID` field has been added to the table that lists attribute mappings.

- The TargetRO attribute has been removed from the definition of the lookup fields reconciliation scheduled task.

  See "Lookup Fields Reconciliation Scheduled Task" on page 4-3 for more information.

- The following are issues resolved in this release:

  > **Note:** Items related to these resolved issues have been removed from the "Known Issues and Limitations" chapter.

Bug Number	Issue	Resolution
6880664	The connector did not support IBM Lotus Notes and Domino Server 8.0.	The connector now supports IBM Lotus Notes and Domino Server 8.0.
6976566	A combination of the First Name and Last Name fields was used to uniquely identify resources in Oracle Identity Manager.	This issue has been resolved. The UniqueID field has been added on the process form for uniquely identifying Lotus Notes resources. This is a read-only field. During a Create User operation, this field is populated with the UniversalID value fetched from the target system at the end of the operation. This field is mapped to the UniversalID field of the target system. If required, you can map the UniqueID field to a different field of the target system. See "Changing the Mapping of the UniqueID Field" on page 3-13 for more information.
6911516	Group description values were not reconciled during group lookup reconciliation runs.	This issue has been resolved. The lookup for groups now contains group names in the Code Key column and group descriptions in the Decode column. If a group does not have a description, then the group name is copied into both the Code Key and Decode columns.
6441230	The simultaneous update of more than one of the following fields was not supported during an Update User provisioning operation: ■ First Name ■ Last Name ■ Middle Name ■ Organizational Unit	This issue has been resolved. You can now update multiple name fields during an Update User provisioning operation.
6925950	During an Update User provisioning operation, all user attributes were sent to the target system even when you changed only some user attributes. This affected performance during the operation.	This issue has been resolved. During an Update User provisioning operation, only user attributes that you change are sent to the target system.

Bug Number	Issue	Resolution
6764284	If you delete a group from the target system, then the group is not removed from the Oracle Identity Manager lookup definition for groups until the next reconciliation run. In earlier releases, if you assigned a user to a deleted group during a provisioning operation, then the user would be assigned to any of the existing groups on the target system. In other words, the group to which the user was assigned on Oracle Identity Manager did not exist on the target system.	This issue has been resolved. Users cannot be assigned to groups that are deleted on the target system.
6909410	If a set of target system records had the same time stamp, then only one of the records from the set was reconciled into Oracle Identity Manager.	This issue has been resolved. All records with time stamp values greater than the time stamp of the last reconciliation run are reconciled.
5616483	When you delete a user on the target system, you can specify the Terminated User group to which the user must be assigned. The connector did not support this feature for provisioning operations.	This issue has been resolved. You can now use the `TerminatedGroupName` IT resource parameter to specify the Terminated User group to which users who are deleted must be assigned. Information about this IT resource parameter has been added in Section 2.2.2, "Configuring the IT Resource.".
7129445	A user was successfully assigned to a group even if the Create User provisioning operation failed.	This issue has been resolved. A user is not assigned to a group if the Create User provisioning operation fails.
7198578	The connector did not support provisioning or reconciliation of multitiered OUs.	This issue has been resolved. The connector now supports provisioning and reconciliation of multitiered OUs.
7318881	The "Out of Back-End Memory" error was encountered during target resource reconciliation of a large number of users.	This issue has been resolved. The Notes document that is created during reconciliation is reused to avoid creation of non-usable Java objects.

Software Updates in Release 9.0.4.5

The following is an issue resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
7482958	In a customized connector, a password set through the Forgot Password feature was not propagated from the OIM User to the Lotus Notes resource.	This issue has been resolved. If you have enabled the propagation of the password from the OIM User to the Lotus Notes resource, then password propagation takes place even when you use the Forgot Password feature.

Software Updates in Release 9.0.4.6

The following is an issue resolved in release 9.0.4.6:

Bug Number	Issue	Resolution
8345014	During Create User and Update User provisioning operations, the full name of the user was not set in the format specified on the target system.	This issue has been resolved. The full name of the user is now set in the format specified on the target system.

Software Updates in Release 9.0.4.7

The following are software updates in release 9.0.4.7:

- Support for New Target System
- MailInternetAddress Added to the List of Reconciled Xellerate User Fields
- Change in Working of the UniqueID Field
- ImmediateDelete and MailFileActionForDelete Parameters Added to the IT Resource
- Resolved Issues in Release 9.0.4.7

Support for New Target System

From this release onward, the connector adds support for IBM Lotus Notes and Domino 8.0.*x*, 8.5 as target systems.

These target system versions are mentioned in the "Verifying Deployment Requirements" section.

MailInternetAddress Added to the List of Reconciled Xellerate User Fields

From this release onward, the MailInternetAddress (Email) field has been added to the list of reconciled Xellerate User fields. See "Reconciled Xellerate User (OIM User) Fields" for more information.

Change in Working of the UniqueID Field

From this release onward, the UniqueID field is not mapped to any field of the target system. Instead, during Create User provisioning operations, the connector creates a unique ID and populates the UniqueID field. The "Changing the Mapping of the UniqueID Field" section has been removed from Chapter 4.

ImmediateDelete and MailFileActionForDelete Parameters Added to the IT Resource

The ImmediateDelete and MailFileActionForDelete parameters have been added to the IT resource. You use the ImmediateDelete parameter to specify how the Delete User provisioning operation must be performed. You use the MailFileActionForDelete parameter to specify how mail file deletion must be performed when a user is deleted.

Resolved Issues in Release 9.0.4.7

The following are issues resolved in release 9.0.4.7:

Bug Number	Issue	Resolution
7557864	An error was encountered while provisioning a Lotus Notes resource to multiple users at the same time.	This issue has been resolved. Multiple users can be provisioned concurrently through the connector.

Bug Number	Issue	Resolution
8215433	The Notes MailIcon name was not changed when the first name or last name was updated.	This issue has been resolved. When the first name, middle name, or last name is updated, the change is propagated to all places on the target system server.
8439171	Reconciliation did not work if you specified a value for the certifierOU parameter in the IT resource.	This issue has now been resolved. Events are reconciled even if you specify a value for the certifierOU parameter.
8471001	Delete User reconciliation events were not linked during target resource reconciliation.	This issue has been resolved. Delete User reconciliation events are now linked during target resource reconciliation.

Software Updates in Release 9.0.4.8

The following are software updates in release 9.0.4.8:

- Support for Reconciliation of Deleted Users
- Resolved Issues in Release 9.0.4.8

Support for Reconciliation of Deleted Users

The Lotus Notes Delete User Reconciliation Task scheduled task has been introduced in this release. You use this scheduled task to reconcile deleted user records. See Section 3.3.4.2, "Scheduled Task for Reconciliation of Deleted Users" for information about this scheduled task.

Resolved Issues in Release 9.0.4.8

The following are issues resolved in release 9.0.4.8:

Bug Number	Issue	Resolution
7356528	When a user account was disabled, it was automatically moved to the default Groups view.	This issue has been resolved. Disabled user accounts are now placed in the Deny Access group.
8634481	The OU part of the user's name fetched from the fullname attribute on the target system was not parsed correctly.	This issue has been resolved. The value fetched from the fullname field is now correctly parsed.
8744907	An unknown response was encountered if the Disable User task was rejected.	This issue has been resolved. A response code has been added for the use case in which the Disable User task is rejected.
8745728	An error was encountered when a scheduled task was configured.	This issue has been resolved. No error is encountered if you correctly configure the scheduled task.
8683657	Reconciliation events are not linked after updating the First Name or Last Name of a target system user record.	This issue has been resolved. Reconciliation events are now linked after updating the First Name or Last Name of a target system user record. **Note:** The Notes Unique ID attribute is used for reconciliation matching.

Software Updates in Release 9.0.4.11

The following are software updates in release 9.0.4.11:

- Addition of IBM Lotus Notes/Domino 8.5.1 to the List of Certified Target Systems
- Universal ID Is Used During Update User Operations

- Inclusion of Javadocs in the Connector Deployment Package
- Resolved Issues in Release 9.0.4.11

Addition of IBM Lotus Notes/Domino 8.5.1 to the List of Certified Target Systems

In this release, IBM Lotus Notes/Domino 8.5.1 has been added to the list of certified target systems. See Section 1.1, "Certified Components" for the full list of target system versions.

Universal ID Is Used During Update User Operations

On the target system, the Universal ID attribute is used to uniquely identify users on the target system. From this release onward, the connector uses the Universal ID during Update User provisioning operations.

Inclusion of Javadocs in the Connector Deployment Package

To facilitate reuse and customization of some parts of the connector code, Javadocs have been included in the connector deployment package.

Resolved Issues in Release 9.0.4.11

The following are issues resolved in release 9.0.4.11:

Bug Number	Issue	Resolution
8521337	The connector failed if you added the Alternate Full Name, Alternate Language, or Alternate Organizational Unit attribute for reconciliation and provisioning.	This issue has been resolved. You can now add the Alternate Full Name, Alternate Language, and Alternate Organizational Unit attributes to the standard set of attributes supported for reconciliation and provisioning. See Chapter 4, "Extending the Functionality of the Connector" for information about the procedure.
8940225	During Create User operations, the connector used the registration server. However, during Update User operations, the connector used the mail server. This caused an error during update operations.	This issue has been resolved. Now, the connector uses either the registration server or the mail server depending on the context.
9398550	The reconciliation of a user's record failed if the record included an attribute that contained the string `OU`.	This issue has been resolved. Records containing the string `OU` are now reconciled.

Software Updates in Release 9.0.4.12

The following are software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for New Target System Version
- Support for Request-Based Provisioning
- Addition of Certifier and Group to the List of Filter Attributes for Reconciliation
- Support for Creation of Lotus User Mail Files in the Background
- Support for Storing Change History for Target System Attributes
- Resolved Issues in Release 9.0.4.12

Support for New Oracle Identity Manager Release

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

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

Support for New Target System Version

From this release onward, the connector supports Lotus Notes version 8.5.2.

See Section 1.1, "Certified Components" for the full list of certified target system versions.

Support for Request-Based Provisioning

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

See Section 3.6.2, "Request-Based Provisioning" for more information.

Addition of Certifier and Group to the List of Filter Attributes for Reconciliation

In earlier releases, you could use the LastName and OU attributes as filter criteria for reconciliation. From this release onward, you can also use the Certifier and Group attributes as filter criteria. See Section 3.3.2, "Limited Reconciliation" for more information.

This item was tracked by Bug 9670080.

Support for Creation of Lotus User Mail Files in the Background

On the target system, you can specify that you want to create mail files in the background during a Create User operation. When you enable this feature, user creation and mail file creation are not part of the same process. From this release onward, the Create Mail DB File In Bckgrnd parameter enables you to select this option. See section on configuring the IT resource in Chapter 2, "Deploying the Connector" for more information.

This item was tracked by Bug 8931359.

Support for Storing Change History for Target System Attributes

From this release onward, the connector supports the target system feature that enables you to store change history for the following attributes:

- Comment
- ShortName
- InternetAddress
- Location
- MailAddress (that is, the ForwardDomain attribute on the target system)

See Chapter 2.3.1.5, "Enabling Storage of Change History for User Attributes" for information about this feature.

This item was tracked by Bug 9558482.

Resolved Issues in Release 9.0.4.12

The following are issues resolved in release 9.0.4.12:

Bug Number	Issue	Resolution
8973747	If there were multiple OU certifiers in your operating environment, then you had to create one IT resource for each certifier.	This issue has been resolved. The certifierOU, CertPath, and CertPwd parameters of the IT resource have been moved to the process form. certifierOU is a lookup field on the process form. During a provisioning operation, you can select a value from this lookup field. In addition, you can enter values in the CertPath and CertPwd fields.
9611834	The Confirm Password field on the process form required users to enter their passwords 2 times.	The Confirm Password field has been removed from the process form.

Software Updates in Release 9.0.4.14

The following are issues resolved in release 9.0.4.14:

Bug Number	Issue	Resolution
9776333	Reconciliation of a large number of user records failed.	This issue has been resolved. No issue is encountered when you reconcile a large number of user records.
10193966	Although an update user provisioning operation failed, a message confirming that the task was successful was displayed.	This issue has been resolved.
10238053	The update user provisioning operation failed if you deployed the connector on Oracle Identity Manager release 9.1.0.1.	This issue has been resolved. The update user provisioning operations no longer fails.

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 9.0.4.4
- Documentation-Specific Updates in Release 9.0.4.5
- Documentation-Specific Updates in Release 9.0.4.6
- Documentation-Specific Updates in Release 9.0.4.7
- Documentation-Specific Updates in Release 9.0.4.8
- Documentation-Specific Updates in Release 9.0.4.11
- Documentation-Specific Updates in Release 9.0.4.12
- Documentation-Specific Updates in Release 9.0.4.14

Documentation-Specific Updates Up to Release 9.0.4.3

The following documentation-specific updates have been made up to release 9.0.4.3:

- In the "Known Issues and Limitations" chapter:
  - The following point has been added:

    "The IBM Lotus Notes and Domino connector can support only one target in secure/SSL mode at a time."
  - The following point has been removed:

No error is thrown if you use Oracle Identity Manager to provision a user account that already exists on IBM Lotus Notes and Domino. This is considered an update operation for the user.

- In the "Deploying the Connector" chapter, the following information has been added:

  The NCSO.jar and the Notes.jar files must also be copied into the *OIM_HOME*/xellerate/ThirdParty directory before the testing utility is used.

Documentation-Specific Updates in Release 9.0.4.4

The following documentation-specific updates have been made in release 9.0.4.4:

- In "Reconciled Resource Object Fields" on page 1-2, the ExpirationDate field has been added.
- In "Adding Standard Target System Attributes for Reconciliation" on page 4-1, the procedure to enable updates of fields that you add for provisioning has been included.
- There are no known issues in this release. Issues related to limitations of the target system have been moved from the "Known Issues and Limitations" chapter to other sections of this guide.

Documentation-Specific Updates in Release 9.0.4.5

There are no documentation-specific updates in release 9.0.4.5.

Documentation-Specific Updates in Release 9.0.4.6

In the "Known Issues and Limitations" chapter, the following known issue has been added:

Bug 8471001

Delete User reconciliation events are not linked during target resource reconciliation.

Documentation-Specific Updates in Release 9.0.4.7

The following documentation-specific updates have been made in release 9.0.4.7:

- Minor corrections have been made in some of the procedures in this guide.
- In the "Known Issues and Limitations" chapter:
  - Two issues tracked by bug numbers 8703999 and 8683657 have been added
  - The following known issue has been deleted:

    Bug 8471001

    Delete User reconciliation events are not linked during target resource reconciliation.

Documentation-Specific Updates in Release 9.0.4.8

Major changes have been made in the structure of the guide. The objective of these changes is to improve the usability of the guide.

Documentation-Specific Updates in Release 9.0.4.11

The following documentation-specific updates have been made in release 9.0.4.11:

- In Section 2.2.2, "Configuring the IT Resource," the description of the RegServer IT resource parameter has been modified.

- Some steps have been added to the procedures described in Section 4.2, "Adding Standard Target System Attributes for Provisioning."
- In the "Known Issues and Limitations" chapter:
  - The issue tracked by the 9490028 bug number has been added.
  - A limitation related to the target system has been added.
  - The following issue has been removed because it is was documented incorrectly as a known issue in the earlier release:

    Bug 8703999

    The value of the IT resource parameter for time stamp does not get updated if you specify a value for the `LastName` filter attribute of the user reconciliation scheduled task.

Documentation-Specific Updates in Release 9.0.4.12

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.14

The following documentation-specific update has been made in revision "15" of release 9.0.4.14:

- The "Oracle Identity Manager" row of Table 1–1, " Certified Components" has been modified.
- Section 1.2, "Usage Recommendation" has been added.

The following documentation-specific updates have been made in the earlier revisions of the release 9.0.4.14:

- In Section 2.2.2, "Configuring the IT Resource," a note has been added in the "ImmediateDelete" and "DenyAccessGroupName" rows of the table.
- In Section 2.3.2.1, "Creating a Deny Access Group," the category to be selected has been added in Step 4. In addition, the group type to be selected has been changed from Multi-purpose to Deny List Only.
- In Chapter 6, "Known Issues and Limitations," a known issue tracked by bug 11693279 has been added.
- In Section 2.3.1.1, "Configuring Trusted Source Reconciliation," the path to locate and download XML files has been updated.
- In Section 1.6.3, "Provisioning Functions," a note has been added to the description of the "Update User Password" function.
- In the "Oracle Identity Manager" row of Table 1–1, " Certified Components", the minimum Oracle Identity Manager release on which this connector can be installed and used has been changed to release 9.1.0.2.
- In Chapter 6, "Known Issues and Limitations," a known issue tracked by bug 16898634 has been added.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use IBM Lotus Notes and Domino either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

Note: At some places in this guide, IBM Lotus Notes and Domino has been referred to as the **target system.**

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

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

Note: It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

This chapter contains the following sections:

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 9.1.0.2 and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector supports. ■ Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1) and future releases in the 11.1.1.*x* series that the connector supports. ■ Oracle Identity Manager 11*g* release 1 PS1 (11.1.1.5.0) and any later BP in this release track
Target systems	IBM Lotus Notes/Domino 6.5, 7.*x*, 8.0.*x*, 8.5, 8.5.1, 8.5.2
External code	NCSO.jar Notes.jar See Section 2.1.3, "Using External Code Files" for more information about these files.
JDK	The JDK version can be one of the following: ■ 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 or a later release in the 1.6 series.

1.2 Usage Recommendation

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

- If you are using an Oracle Identity Manager release that is 9.1.0.1 or later and earlier than Oracle Identity Manager 11*g* Release 1 (11.1.1.5.4), then use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.4) or later, or Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later then use the latest 11.1.1.*x* version of this connector.
- If the IBM Lotus Notes and Domino target systems are deployed on any of the following operating system platforms, then use the latest 11.1.1.*x* version of this connector:
  - Oracle Enterprise Linux later than 5.2+x86 (32-bit) and x64 (64-bit)
  - Solaris 11

1.3 Certified Languages

The connector supports the following languages:

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

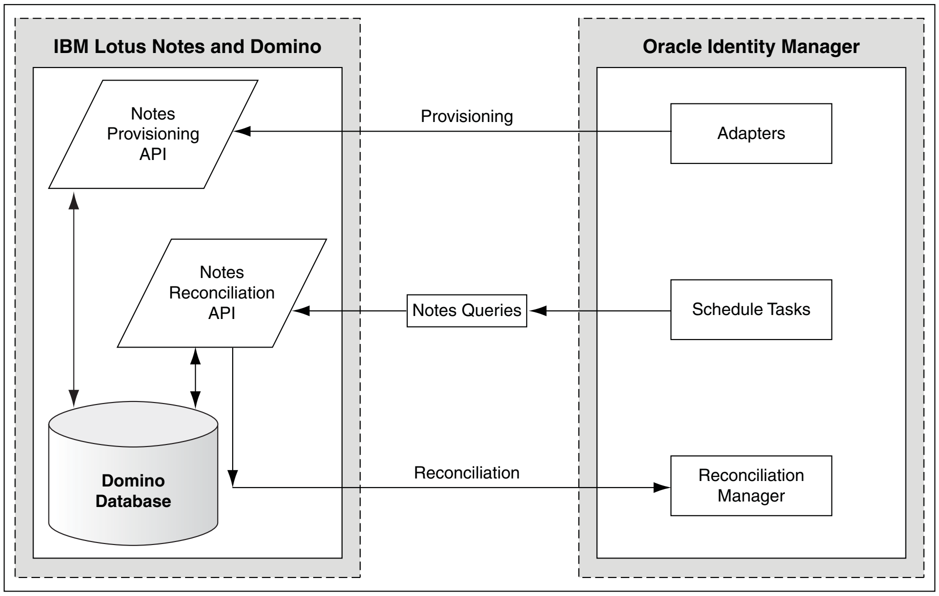
See Also: For information about supported special characters:

- For Oracle Identity Manager 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*.

1.4 Connector Architecture

Figure 1–1 shows the architecture of the connector for IBM Lotus Notes and Domino.

Figure 1–1 Architecture of the Connector



Note: The connector does not use the Certificate Authority (CA) process.

The connector can be configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this form of reconciliation, OIM Users are created or updated corresponding to the creation of and updates to users on the target system.

- Account Management

  Account management is also known as target resource management. This mode of the connector enables the following operations:

  - Provisioning

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

  - Target resource reconciliation

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

    Note: In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term scheduled task used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term scheduled job in the context of Oracle Identity Manager release 11.1.1.

    See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

1.5 Features of the connector

This section discusses the following topics:

- Section 1.5.1, "Support for Both Target Resource and Trusted Source Reconciliation"
- Section 1.5.2, "Support for Limited Reconciliation"
- Section 1.5.3, "Support for Batched Reconciliation"
- Section 1.5.4, "Support for Reconciliation of Deleted User Records"
- Section 1.5.5, "Support for Both Full and Incremental Reconciliation"
- Section 1.5.6, "Support for Adding New Single-Valued Attributes for Reconciliation and Provisioning"

1.5.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure Oracle Internet Directory as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3, "Configuring Reconciliation" for more information.

1.5.2 Support for Limited Reconciliation

For a reconciliation run, you can specify the subset of added or modified target system records that must be reconciled.

See Section 3.3.2, "Limited Reconciliation" for more information.

1.5.3 Support for Batched Reconciliation

Batched reconciliation is the reconciliation of a specified number of target system records at a time, within a reconciliation run. Multiple batches of records are fetched to complete the reconciliation run. This feature helps reduce memory issues that might arise when there are a large number of records to be reconciled.

See Section 3.3.3, "Batched Reconciliation" for more information.

1.5.4 Support for Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records. In target resource mode, if a record is deleted on the target system, then the corresponding IBM Lotus Notes and Domino resource is revoked from the OIM User. In trusted source mode, if a record is deleted on the target system, then the corresponding OIM User is deleted.

See Section 3.3.4.2, "Scheduled Task for Reconciliation of Deleted Users" for more information about scheduled tasks used for reconciling deleted user records.

1.5.5 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, change-based or incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time.

See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for more information.

1.5.6 Support for Adding New Single-Valued Attributes for Reconciliation and Provisioning

You can add to the standard set of single-valued attributes for reconciliation and provisioning. Chapter 4, "Extending the Functionality of the Connector" describes the procedure.

1.6 Connector Objects Used in the Target Resource Mode

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about reconciliation configurations

This section discusses the following topics:

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Lookup Definitions"

- Section 1.6.3, "Provisioning Functions"
- Section 1.6.4, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–2 provides information about user attribute mappings for target resource reconciliation and provisioning.

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

Process Form Field	IBM Lotus Notes and Domino Attribute	Description
First Name	FirstName	First name
Middle Name	MiddleInitial	Middle name
Last Name	LastName	Last name
Short Name	ShortName	Short name
Password	UserPassword	Password
Security Type	License	Security type for user (North American or International)
End Date	ExpirationDate	Expiration date of certificate
Organizational Unit	OU	Organization to which user belongs
Mail Internet Address	InternetAddress	E-mail address.
Location	Location	Location
Comment	Comment	Comment
Forward Domain	MailAddress	Forwarding e-mail address
GRP Name	GROUPLIST	Group to which user belongs
UniqueID	Full hierarchical name of a user	Full hierarchical name that uniquely identifies each user account on the target system. For example: G=*FIRST_NAME*/I=*MIDDLEINITIAL*/S=LASTNAME/CN=FIRSTNAME MIDDLEINITIAL LASTNAME/OU=ORGANIZATIONUNIT/O=ORGANIZATION
Universal ID	Universal Id	16-bit alphanumeric ID that uniquely identifies a user **Note:** At the end of a Create User provisioning operation, the Universal Id is created on the target system and then fetched to Oracle Identity Manager.

1.6.2 Lookup Definitions

The Lookup.Lotus.Grp lookup definition is used to hold values for the Group lookup field on the process form. Similarly, the Lookup.Lotus.OU lookup definition is used to hold values for the OU lookup field on the process form. Lookup field synchronization involves fetching group and OU names from the target system and storing them in these lookup definitions.

1.6.3 Provisioning Functions

Table 1–3 lists the provisioning functions that are available with this connector.

Table 1–3 Provisioning Functions

Function	Description	Adapter
Create User	Creates a user	LNCreateUser
Delete User	Deletes a user **Note:** This function is implemented using the DeleteUser Administration Process (AdminP) function of IBM Lotus Notes and Domino.	LNDeleteUser
Update User Last Name	Updates the last name of a user **Note:** This function is implemented using the RenameNotesUser AdminP function of IBM Lotus Notes and Domino.	LNUpdateUserName
Update User First Name	Updates the first name of a user **Note:** This function is implemented using the RenameNotesUser AdminP function of IBM Lotus Notes and Domino.	LNUpdateUserName
Update User Middle Name	Updates the middle name of a user **Note:** This function is implemented using the RenameNotesUser AdminP function of IBM Lotus Notes and Domino.	LNUpdateUserName
Update User Organizational Unit	Updates the organizational unit of a user **Note:** This function is implemented using the RenameNotesUser AdminP function of IBM Lotus Notes and Domino.	LNUpdateUserName
Update User Short Name	Updates the short name of a user	LNUpdateUserInfo
Update User Mail Internet Address	Updates the e-mail address of a user	LNUpdateUserInfo
Update User Location	Updates the location of a user	LNUpdateUserInfo
Update User Comment	Updates the comment of a user	LNUpdateUserInfo
Update User Forward Domain	Updates the e-mail address to which e-mail for the user must be forwarded	LNUpdateUserInfo
Update User Password	Updates the user password and resets (or updates) the ID file **Note:** This connector changes password only in Lotus Notes. If the password synchronization between Lotus Notes and Domino Internet/HTTP passwords is not enabled, then the password change made from Oracle Identity Manager to Lotus Notes is not reflected in the Internet/HTTP password. To synchronize passwords between Lotus Notes and Domino Internet/HTTP: ■ Enable the password synchronization feature in the target system. ■ Set the sync flag to "true" in the user record.	LNUpdatePassword
Disable User	Disables a user	LNEnableDisable
Enable User	Enables a user	LNEnableDisable

1.6.4 Reconciliation Rule for Target Resource Reconciliation

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

The following is the process matching rule:

Rule name: Reconcile Lotus User

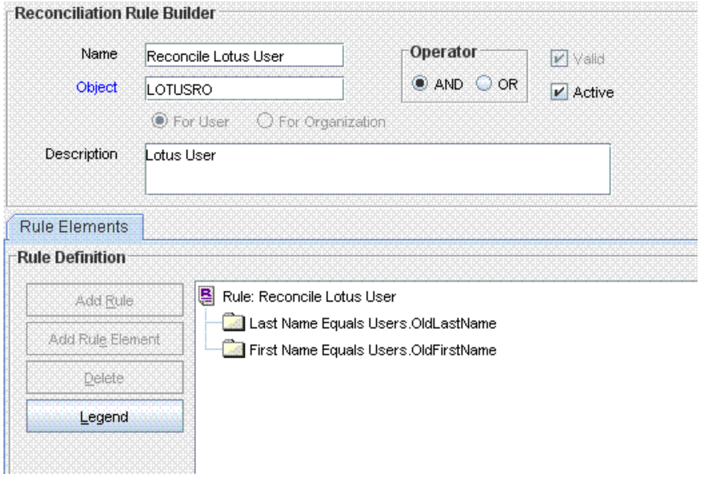
Rule element: (Last Name Equals Users.OldLastName) AND (First Name Equals Users.OldFirstName)

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

> **Note:** Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Reconcile Lotus User**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



Name: Reconcile Lotus User

Object: LOTUSRO

● For User ○ For Organization

Description: Lotus User

Operator: ● AND ○ OR

☑ Valid

☑ Active

Rule: Reconcile Lotus User

Last Name Equals Users.OldLastName

First Name Equals Users.OldFirstName

1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–4 lists the action rules for target resource reconciliation.

Table 1–4 Action Rules for Target Resource Reconciliation

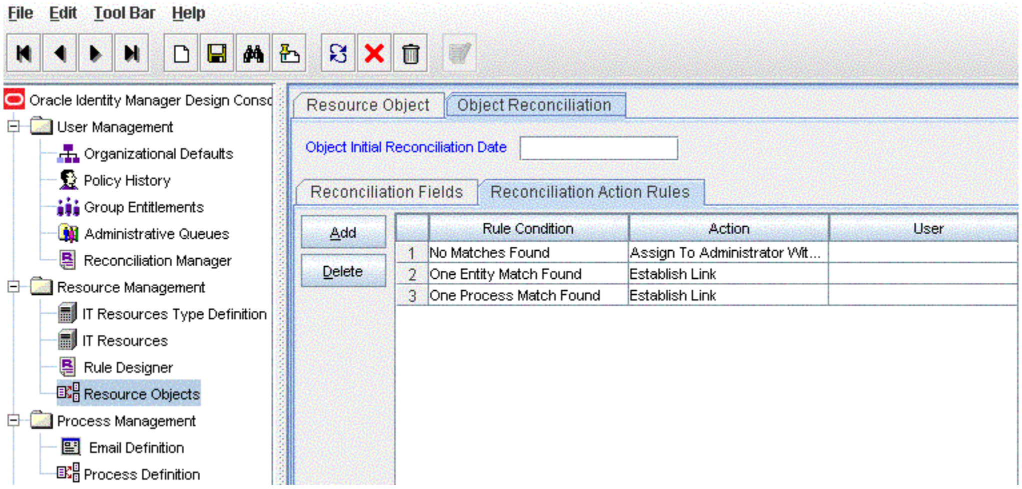
Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

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

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **LOTUSRO** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



	Rule Condition	Action	User
1	No Matches Found	Assign To Administrator Wit...	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.7 Connector Objects Used in the Trusted Source Mode

This section discusses the following topics:

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–5 lists attribute mappings for trusted source reconciliation.

Table 1–5 User Attributes for Trusted Source Reconciliation

OIM User Form Field	IBM Lotus Notes and Domino Attribute
User ID	LastName
First Name	FirstName
Last Name	LastName
Employee Type	Full-Time
User Type	End-User
Organization	XellerateOrganization
Email	InternetAddress

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

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

The following is the process matching rule:

Rule name: Lotus Notes XellerateUser Rule

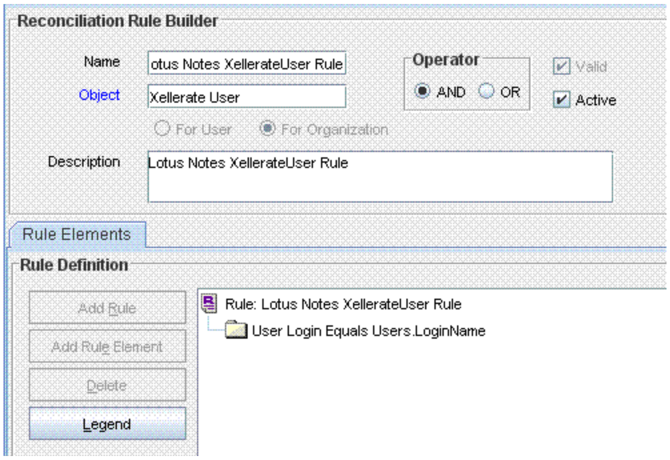
Rule element: User Login Equals Users.LoginName

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

Note: Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Lotus Notes XellerateUser Rule**. Figure 1–4 shows the reconciliation rule for target resource reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



Name: otus Notes XellerateUser Rule

Object: Xellerate User

○ For User ● For Organization

Description: Lotus Notes XellerateUser Rule

Operator: ● AND ○ OR

☑ Valid

☑ Active

Rule: Lotus Notes XellerateUser Rule

User Login Equals Users.LoginName

1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–6 lists the action rules for trusted source reconciliation.

Table 1–6 Action Rules for Trusted Source Reconciliation

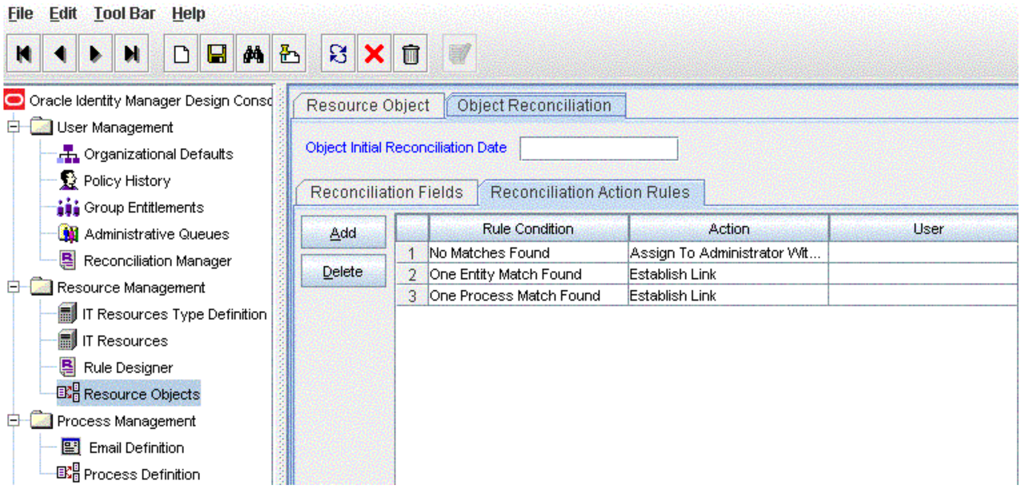
Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

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

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rule for target resource reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



	Rule Condition	Action	User
1	No Matches Found	Assign To Administrator Wit...	
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

1.8 Roadmap for Deploying and Using the Connector

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

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.
- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" describes the procedure to test the connector.
- Chapter 6, "Known Issues and Limitations" lists known issues associated with this release of the connector.

2 Deploying the Connector

The procedure to deploy the connector can be divided into the following stages:

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

This section is divided into the following topics:

- Section 2.1.1, "Files and Directories on the Installation Media"
- Section 2.1.2, "Determining the Release Number of the Connector"
- Section 2.1.3, "Using External Code Files"
- Section 2.1.4, "Creating a Target System Account for Connector Operations"

2.1.1 Files and Directories on the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
config/adminP.properties	This file is used to specify a value for an AdminP command that is run on the Domino server.
configuration/IBM Lotus Notes Domino-CI.xml	This XML file contains configuration information that is used during connector installation.
config/attributemapping_prov.properties	This file contains the parameters required for provisioning.
config/attributemapping_recon.properties	This file contains the parameters required for reconciliation.
Files in the dataset directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
lib/xlLotusNotesProvision.jar	This JAR file contains the class files that are used to implement provisioning. During connector deployment, this file is copied to the following location: - For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks - For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database

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

File in the Installation Media Directory	Description
lib/xlLotusNotesRecon.jar	This JAR file contains the class files that are used to implement reconciliation. During connector deployment, this file is copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector deployment, these resource bundles are copied to the following location: ■ For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
test/config/log.properties	This file is used to specify the log level and the directory in which the log file is to be created when you run the testing utility.
test/config/config.properties	This file is used to specify the parameters and settings required to connect to the target system by using the testing utility.
test/scripts/lotusNotes.bat	This file contains the script required for running test calls from the Oracle Identity Manager server on Microsoft Windows platforms.
test/scripts/lotusNotes.sh	This file contains the script required for running test calls from the Oracle Identity Manager server on UNIX-based platforms.
test/config/config_unid.properties	This file is used to store the value of the `UniqueID` user attribute while using the testing utility. Section 5.1, "Testing the Connector" provides information about using this file.
xml/xlLotusNotes_XellerateUser.xml	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.
xml/xlLotusNotesConnector.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Resource object ■ Process definition ■ Process tasks ■ Adapters ■ Process form ■ Lookup definitions

2.1.2 Determining the Release Number of the Connector

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

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

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME/xellerate/JavaTasks/xlLotusNotesRecon.jar

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

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

2.1.3 Using External Code Files

> **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 contents of the connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.

Copy the following files into the *JAVA_HOME*/jre/lib/ext directory:

- NCSO.jar from the *LOTUS_HOME*/lotus/Domino/data/domino/java directory
- Notes.jar from the *LOTUS_HOME*/Domino/jvm/lib/ext directory

Here, java_installation is the JDK directory used for Oracle Identity Manager and *LOTUS_HOME* is the directory in which IBM Lotus Notes and Domino is installed.

Section 5.1, "Testing the Connector" describes the procedure to use the testing utility. Before running the testing utility, copy the NCSO.jar and Notes.jar files into the following directory:

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

  OIM_HOME/xellerate/ThirdParty

- For Oracle Identity Manager release 11.1.1:

  OIM_HOME/server/ThirdParty

2.1.4 Creating a Target System Account for Connector Operations

Oracle Identity Manager uses a target system user account to provision to and reconcile data from the target system. For IBM Lotus Notes and Domino, this target system account must be a full access administrator account. See the target system documentation for creating an account of this type.

While performing the procedure described in Section 2.2.2, "Configuring the IT Resource," you specify the credentials of the administrator account as the values of the Admin and AdminPwd parameters.

2.2 Installation

> **Note:** 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.

Installing the connector involves the following procedures:

- Section 2.2.1, "Running the Connector Installer"
- Section 2.2.2, "Configuring the IT Resource"

2.2.1 Running the Connector Installer

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 **IBM Lotus Notes Domino *RELEASE_NUMBER***. This list displays the names and release numbers of

connectors whose installation files you copy into the default connector installation directory:

OIM_HOME/xellerate/ConnectorDefaultDirectory

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

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

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

c. From the Connector List list, select **IBM Lotus Notes Domino *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 Target Resource user configuration XML file (by using the Deployment Manager).

   c. Compilation of adapters

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. 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 PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.1.3, "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 Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

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

8. Copy the files in the config directory on the installation media to the *OIM_HOME*/xellerate/XLIntegrations/LotusNotes/config directory.

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

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Table 2–1 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.2.2 Configuring the IT Resource

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

1. Log in to the Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   - On the Welcome page, click **Advanced** in the upper-right corner of the page.
   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter `LotusNotes` and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. Table 2–2 describes each parameter.

Table 2–2 Parameters of the IT Resource

Parameter	Description
AddBook	Enter `True` if you want the server entry in the Domino Directory to be updated when the ID file is created. Otherwise, enter `False`. The default value is `True`. **Note:** The Domino Directory is the database that contains user personal documents, connection documents, server documents, and cross-certification files. This directory is also known as the public address book or names.nsf.
Admin	Enter the user ID of the administrator account that you create by performing the procedure described in Section 2.1.4, "Creating a Target System Account for Connector Operations."
AdminPwd	Enter the password of the administrator account that you create by performing the procedure described in Section 2.1.4, "Creating a Target System Account for Connector Operations."
Create Mail DB File	Enter `True` if you want a mail file to be created with the ID file when the Register New User function of IBM Lotus Notes and Domino is called. Otherwise, enter `False`. The default value is `True`.
Create Mail DB File In Bckgrnd	Enter `True` if you want the mail file to be created in the background. Otherwise, enter `False`. The default value is `False`. This parameter is taken into consideration only if the value of the Create Mail DB File parameter is `True`. **Note:** If you enter `True` as the value, then the connector cannot verify whether mail files are successfully created during Create User provisioning operations.
Host	Enter the host name or IP address of the IBM Lotus Notes and Domino server.
Port	Enter the TCP/IP port at which the IBM Lotus Notes and Domino server is listening. The default value is `63148`.
IDFilePath	Enter the path for storing ID files.
IDType	Enter the type of ID files to be created. The value can be `172` (for HIERARCHICAL) or `173` (for CERTIFIER). The default value is `172`.
MailDBPath	Enter the mail file path.
MailOwnerAccess	Enter the mail database ACL setting for the owner. The value can be one of the following: ■ `0` (for MANAGER) ■ `1` (for DESIGNER) ■ `2` (for EDITOR) The default value is `0`.
MailQuotaLimit	Enter the maximum size of the user's e-mail database, in megabytes. The default value is `50`.
MailQuotaWarning	Enter the size, in megabytes, at which the user's mail database issues a warning that the size limit may be exceeded. The default value is `40`.
MailServer	Enter the canonical name of the server containing the user's mail file. Sample value: `CN=ServerName/O=OrgName` **Note:** You must enter a value for this parameter.

Table 2–2 (Cont.) Parameters of the IT Resource

Parameter	Description
MailSystem	Specify the type of user's mail system. The value can be any one of the following: ■ 0 (for NOTES) ■ 3 (for INOTES) ■ 4 (for INTERNET) The default value is 0.
MailTemplateName	Enter the name of the template for the mail file.
PasswordLength	Enter the minimum number of characters that can be used in the password. The value can be any number. The default minimum length is 5.
RegLog	Enter the name of the log file to be used when creating IDs. The default value is `log.nsf`.
RegServer	Enter the canonical name of the server to be used when creating IDs and performing other registration functions. Sample value: `CN=MyServer/O=MyOrg`
StoreAddBook	Enter `True` to specify that the ID file is stored in the Domino Directory of the server. Otherwise, enter `False`. The default value is `True`.
Sync Internet Password	Enter `True` to specify that the user can use the same password for both local client-based access and Web-based access to IBM Lotus Notes and Domino. Otherwise, enter `False`. The default value is `True`.
IsSecure	Enter `Yes` to specify that the SSL feature is enabled. Otherwise, enter `No`. The default value is `Yes`. **Note:** It is recommended that you enable SSL to secure communication between Oracle Identity Manager and the target system.
DenyAccessGroupName	Enter the name of the group for users whose accounts have been disabled. **Note:** - If there is no Deny Access group on the IBM Lotus Notes and Domino installation, then you must create one by performing the procedure described in the "Creating a Deny Access Group" section on page 2-20. - If the target system contains more than one Deny Access group and you don't specify a value for the DenyAccessGroupName parameter, then disabled users automatically become members of the first Deny Access group that the connector finds.
triggerAdminp	Enter `Yes` to specify that the Trigger AdminP feature is enabled. Otherwise, enter `No`. The default value is `Yes`.
isAgentInstalled	Enter `Yes` if you want to enable support for encrypted e-mail on the target system. Otherwise, enter `No`. **See Also:** The "Enabling Modification of ID Files" section on page 2-21 for more information about this parameter.
TrustedTimeStamp	This parameter is used for trusted source reconciliation. Starting with the first reconciliation run, this parameter stores the time stamp at which the reconciliation run ends. The default value is `None`. You can set the value to `None` whenever you want to perform a full reconciliation run. See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for more information.

Table 2–2 (Cont.) Parameters of the IT Resource

Parameter	Description
NonTrustedTimeStamp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time stamp at which the reconciliation run ends. The default value is `None`. You can set the value to None whenever you want to perform a full reconciliation run. See Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation" for more information.
Max Retries	Enter the number of times that the connector must retry connecting to the target server, in case the connection fails. The default value is `2`.
Delay	Enter the delay (in milliseconds) before the connector must retry connecting to the target system, in case the connection fails. The default value is `10000`.
TerminatedGroupName	Enter the name of the Terminated User group to which users who are deleted must be assigned.
ImmediateDelete	Use this parameter to specify how the Delete User provisioning operation must be performed. You can specify one of the following values: ■ Enter `Yes` if you want all references to the user (except for the mail and ID files) in the Domino Directory to be deleted before an administration process request is issued. **Note:** - A mail file is deleted *only* after the administrator approves the administration process request. - Deletion of ID files is not supported. ■ Enter `No` if you want to let the administration process make all required deletions. The default value is `Yes`.
MailFileActionForDelete	Use this parameter to specify how mail file deletion must be performed when a user is deleted. You can specify one of the following values: ■ Enter `Delete All` if you want the mail file on the user's home server and all replicas of the mail file to be deleted. ■ Enter `Delete Home` if you want the mail file on the user's home server to be deleted. ■ Enter `Delete None` if you do not want the user's mail file to be deleted. The default value is `Delete All`.
User Info Update History Required	Enter `Yes` to specify that history must be maintained for attributes such as short name, internet address, location, forward domain and comment attributes. Otherwise, enter `No`. The default value is `Yes`. See Section 2.3.1.5, "Enabling Storage of Change History for User Attributes" for more information about this parameter.
Configuration Lookup	This parameter is used to store the name of the configuration lookup definition. Default value: `Lookup.Lotus.Configurations` **Note:** See Section 2.3.1.5, "Enabling Storage of Change History for User Attributes" for information about this lookup definition. If you create another lookup definition to store connector configuration parameters, then specify the name of the new lookup definition as the value of this parameter.

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

2.3 Postinstallation

The following sections discuss postinstallation procedures:

- Section 2.3.1, "Configuring Oracle Identity Manager"
- Section 2.3.2, "Configuring the Target System"
- Section 2.3.3, "Configuring SSL"

2.3.1 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

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

- Section 2.3.1.1, "Configuring Trusted Source Reconciliation"
- Section 2.3.1.2, "Changing to the Required Input Locale"
- Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.1.4, "Enabling Logging"
- Section 2.3.1.5, "Enabling Storage of Change History for User Attributes"
- Section 2.3.1.6, "Enabling Request-Based Provisioning"

2.3.1.1 Configuring Trusted Source Reconciliation

You can configure the connector to designate the target system as a target resource or trusted source.

> **Note:** You can skip this section if you do not want to designate the target system as a trusted source for reconciliation. As mentioned earlier in this guide, it is recommended that you do not configure the target system as both a trusted source and target resource.

The following is a summary of the steps involved in configuring trusted source reconciliation:

1. Import the XML file for trusted source reconciliation, xlLotusNotes_XellerateUser.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 xlLotusNotes_XellerateUser.xml file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Specify values for the attributes of the Lotus Notes trusted User Reconciliation scheduled task. This procedure 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 Oracle Identity Manager release 9.1.0.*x*, then:
   1. Click the **Deployment Management** link on the left navigation bar.
   2. 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:
   1. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   2. 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 xlLotusNotes_XellerateUser.xml file located in the following directory:
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory/IBM_Lotus_9.0.4.14.0/xm l
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/IBM_Lotus_9.0.4.14.0/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**.

2.3.1.2 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.

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.1.0.*x* and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

For Oracle Identity Manager release 9.1.0.*x*:

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

For Oracle Identity Manager release 11.1.1:

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

---

2. Enter one of the following commands:

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

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

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

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

  On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`

  On UNIX: `PurgeCache.sh ConnectorResourceBundle`

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

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

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

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

  In this format:

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

  - Replace `OIM_PORT_NUMBER` with the port on which Oracle Identity Manager is listening.

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

2.3.1.4 Enabling Logging

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

- Section 2.3.1.4.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.1.4.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.3.1.4.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.*x*

> **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 might 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:

- **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.ADAPTER.LOTUSNOTES=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.ADAPTER.LOTUSNOTES=INFO
   ```

After you enable logging, log information is displayed on the server console.

- **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.ADAPTER.LOTUSNOTES=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.ADAPTER.LOTUSNOTES=INFO
     ```

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

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

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

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

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

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

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

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

     ```
     log4j.logger.XELLERATE=log_level
     log4j.logger.XL_INTG.LOTUSNOTES=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.LOTUSNOTES=INFO
     ```

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

  ORACLE_HOME/opmn/logs/default_group~home~default_group~1.log

2.3.1.4.2 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 2–3.

Table 2–3 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='lotusnotes-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="ADAPTER.LOTUSNOTES" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="lotusnotes-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 2–3 lists the supported message type and level combinations.

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

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

```
<log_handler name='lotusnotes-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="ADAPTER.LOTUSNOTES" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="lotusnotes-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.

2.3.1.5 Enabling Storage of Change History for User Attributes

> **Note:** This section describes an optional procedure. Perform this procedure only if you want to enable storing of change history for some user attributes on the target system.

You use the HISTORY_REQUIRED_FOR_ATTRIBUTES entry of the Lookup.Lotus.Configurations lookup definition to specify the attributes for which the target system must maintain change history. You can specify any combination of the following attributes:

- ShortName
- InternetAddress
- Location
- MailAddress (that is, the ForwardDomain attribute on the target system)
- Comment

To specify the attributes for which change history must be maintained:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.

2. Search for and open the **Lookup.Lotus.Configurations** lookup definition.
3. In the Decode column for the **HISTORY_REQUIRED_FOR_ATTRIBUTES** entry, enter any combination of the following attributes in a comma-delimited list:
   - ShortName
   - Location
   - InternetAddress
   - MailAddress (that is, the ForwardDomain attribute on the target system)
   - Comment

   For example: `ShortName,InternetAddress,MailAddress`
4. Click the Save icon.

2.3.1.6 Enabling Request-Based Provisioning

> **Note:** The feature described in this section is supported only on Oracle Identity Manager release 11.1.1. Perform the procedure described in this section only if you want to enable request-based provisioning.

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

> **Note:** Direct provisioning cannot be used if you enable request-based provisioning.

Enabling request-based provisioning involves performing the following procedures:

- Section 2.3.1.6.1, "Copying Predefined Request Datasets"
- Section 2.3.1.6.2, "Importing Request Datasets into the MDS"
- Section 2.3.1.6.3, "Enabling the Auto Save Form Feature"
- Section 2.3.1.6.4, "Running the PurgeCache Utility"

2.3.1.6.1 Copying Predefined Request Datasets

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

- ProvisionResource_LOTUSRO.xml
- ModifyProvisionedResource_LOTUSRO.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\LotusNotes

> **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.

2.3.1.6.2 Importing Request Datasets into the MDS

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

To import a request dataset definition into the MDS:

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

   > **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.3.1.6.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\LotusNotes 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 values for the following:
   - `Please enter your username [weblogic]`

Enter the user name used to log in to Oracle WebLogic Server.

Sample value: `WL_User`

- `Please enter your password [weblogic]`

  Enter the password used to log in to Oracle WebLogic Server.

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

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

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

  In this format, replace:

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

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

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

/custom/connector/*RESOURCE_NAME*

2.3.1.6.3 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 **LOTUSRO** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.1.6.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.1.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.3.2 Configuring the Target System

Configuring the target system involves performing the following steps:

- Section 2.3.2.1, "Creating a Deny Access Group"
- Section 2.3.2.2, "Enabling Modification of ID Files"
- Section 2.3.2.3, "Additional Functionality Changes Related to the ID Files"
- Section 2.3.2.4, "Ensuring That the Domino IIOP (DIIOP) Task Is Running"

2.3.2.1 Creating a Deny Access Group

When you disable a user account in IBM Lotus Notes and Domino, that user automatically becomes a member of a Deny Access group. When you reenable the user account, the user is removed from the Deny Access group. The same process is followed when you disable a user account through Oracle Identity Manager. For the Disable User operation to work, there must be at least one Deny Access group in the target system.

If there is no Deny Access group on the IBM Lotus Notes and Domino installation, then you must create one as follows:

1. Log in to the Lotus Notes client as the administrator.
2. On the People & Groups tab, click the **Groups** folder on the left pane.
3. Click **Add Group**.
4. On the New Group tab, provide the following values:
   - **Category**: Select **Administration along with.**
   - **Group name**: Specify a name for the group, for example, `noaccess`.
   - **Group type**: Select **Deny List Only**.
5. Click **Save & Close**.
6. On the Configuration tab, click **All Server Documents** on the left pane.
7. On the right pane, double-click the row for the server that you are using.
8. Open the Security tab.
9. In the Server Access section, double-click **Not Access Server**.
10. In the Select Names dialog box, use the **Add** button to add the group that you create in Step 4 and then click **OK**.
11. Click **Save & Close**.

The Deny Access group that you create can be viewed by performing Steps 6 through 9.

While configuring the IT resource, you specify the name of the Deny Access group (for example, `noaccess`) that you create in Step 4 as the value of the DenyAccessGroupName IT resource parameter.

2.3.2.2 Enabling Modification of ID Files

> **Note:** If you do not want to support encrypted e-mail on the target system, then you can skip this section.

When you create a user account in IBM Lotus Notes and Domino, an ID file is automatically generated for the user account. This ID file holds the encryption key for the user, and it is automatically used when encrypted e-mail is sent or received.

If an administrator changes the user's password in Oracle Identity Manager, then a new ID file is created. This new ID file cannot be used to open existing sent and received encrypted e-mail. From this point onward, existing encrypted e-mail becomes inaccessible.

To avoid this situation:

1. Configure an agent on IBM Lotus Notes and Domino that modifies existing ID files when the password is updated. This section describes the procedure to configure an agent.
2. Set the value of the isAgentInstalled IT resource parameter to `Yes` to indicate that an agent has been configured on IBM Lotus Notes and Domino. This parameter is described later in this guide.

To configure the agent on IBM Lotus Notes and Domino:

1. Log in to the Lotus Domino Administrator client.
2. Depending on the target system version that you use, perform one of the following steps:
   - For IBM Lotus Notes and Domino Server 6.5, 7.*x*:

     From the **File** menu, select **Database** and then select **Open.**
   - For IBM Lotus Domino Server 8.0.*x*, and 8.5:

     From the **File** menu, select **Application** and then select **Open.**
3. In the Open Database dialog box, select the name of the Domino server from the Server list.
4. In the **FileName** field, enter `names.nsf` and then click **Open**.

   > **Note:** The IBM Lotus Notes Domino connector does not support multiple Notes Address Books. Only the default address book (names.nsf) is supported.

5. From the **View** menu, select **Agents**.
6. Click **New Agent**.
7. On the first tab of the Agent dialog box (indicated by a bulb icon), enter the following values:

   Name: Enter `changePassword`.

   Comment: Enter `Change password of the ID file`.

   Target: Select **All documents in database**.
8. On the second tab of the Agent dialog box (indicated by a key icon), select **Allow restricted operations** from the **Set runtime security level** list.
9. Close the dialog box.
10. On the changePassword-Agent tab, select **LotusScript** from the second list.
11. From the menu on the Objects pane, select the **[Options]** method.
12. Open the following file in the installation media directory:

    script/lotusagent.txt
13. Copy the LotusScript code from the lotusagent.txt file to the right pane of the Lotus Notes client window.
14. From the **File** menu, select **Save**.

You specify the credentials of a Lotus Notes administrator account in the IT resource definition. After you configure the agent on IBM Lotus Notes and Domino, you must ensure that this Lotus Notes administrator account has the permissions required to update the ID files as follows:

1. Log in to the Lotus Domino Administrator client.
2. Depending on the target system version that you use, perform one of the following steps:
   - For IBM Lotus Notes and Domino Server 6.5, 7.*x*:

     From the **File** menu, select **Database** and then select **Open.**

- For IBM Lotus Domino Server 8.0.*x*, 8.5:

  From the **File** menu, select **Application** and then select **Open.**

3. Select the Lotus Notes administrator account that you are using to connect to the Domino server.
4. In the Access Control List dialog box, select **Manager** from the **Access** list and then select the **Delete documents** check box.
5. Click **OK**.

2.3.2.3 Additional Functionality Changes Related to the ID Files

The following fields have been added on the user process form:

- **ID File Name**

  You can use the ID File Name field to specify a name for the ID file while creating a user account.

- **Old Password**

  The Old Password field stores the latest password of the user in encrypted form. The value of this field is changed automatically during Create Password and Update Password provisioning operations.

> **Note:** After reconciliation, for user accounts for which the password has been changed on the target system, the users must manually enter the new password in this field on Oracle Identity Manager.

2.3.2.4 Ensuring That the Domino IIOP (DIIOP) Task Is Running

To ensure that the Domino IIOP (DIIOP) task is running, open the IBM Lotus Notes and Domino console and run the Load DIIOP command.

If the DIIOP task was not running, then it is started after you run the command. If it was running, then a message that the task has already been started is displayed.

2.3.3 Configuring SSL

> **Note:**
>
> - This is an optional step of the deployment procedure. For more information about this procedure, see
>
>   `http://www-128.ibm.com/developerworks/lotus/library/ls-Java_access_2/`
>
> - The connector can support only one target system installation in secure/SSL mode at a time.

To set up SSL connectivity between Oracle Identity Manager and the IBM Lotus Notes and Domino server:

1. Ensure that the DIIOP and HTTP tasks are running on the IBM Lotus Notes and Domino server for SSL communication.

> **Note:** If you have already performed the procedure described in the "Configuring the Target System" section on page 2-20, then the DIIOP task is already running.

2. On the IBM Lotus Notes and Domino server, create a key ring using the Server Certificate Admin (certsrv.nsf) database. Move the two key ring files, keyfile.kyr and keyfile.sth, to the data directory of the server.
3. Restart the DIIOP task to generate a file named `TrustedCerts.class` in the IBM Lotus Notes and Domino data directory. The following is the typical path where this file may be found:

   LOTUS_HOME/Domino/data/domino/java

   Here, *LOTUS_HOME* is the directory in which IBM Lotus Notes and Domino is installed.
4. Package the TrustedCerts.class file in the TrustedCerts.jar file.
5. Move the TrustedCerts.jar file to the *JAVA_HOME*\jre\lib\ext directory on Oracle Identity Manager host. Here, *JAVA_HOME* is the JDK installation directory that is used by Oracle Identity Manager.

3

Using the Connector

This chapter is divided into the following sections:

- Section 3.1, "Performing First-Time Reconciliation"
- Section 3.2, "Scheduled Task for Lookup Field Synchronization"
- Section 3.3, "Configuring Reconciliation"
- Section 3.4, "Configuring Scheduled Tasks"
- Section 3.5, "Guidelines on Performing Provisioning"
- Section 3.6, "Performing Provisioning Operations"
- Section 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"
- Section 3.8, "Guidelines on Performing Reconciliation"

3.1 Performing First-Time Reconciliation

After you deploy the connector, you must first reconcile all existing target system user records into Oracle Identity Manager. The following is a summary of the procedure:

> **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.
>
> See Section 3.4, "Configuring Scheduled Tasks" for information about the procedure to configure scheduled tasks.

- If you are using the target system as a target resource, then:

  1. Configure and run the Lotus Notes Lookup Reconciliation scheduled task to synchronize lookup field values. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about the attributes of this scheduled task.
  2. Configure and run the Lotus Notes User Reconciliation scheduled task to reconcile user records from the target system. See Section 3.3.4.1, "Scheduled

Tasks for Reconciliation of User Records" for information about the attributes of this scheduled task.

Reconciled user records are converted into Lotus Notes resources assigned to OIM Users.

- If you are using the target system as a trusted source, then configure and run the Lotus Notes Trusted User Reconciliation scheduled task to reconcile user records from the target system. See Section 3.3.4.1, "Scheduled Tasks for Reconciliation of User Records" for information about the attributes of this scheduled task.

  Reconciled user records are converted into OIM Users.

3.2 Scheduled Task for Lookup Field Synchronization

The Lotus Notes Lookup Reconciliation scheduled task is used for lookup field synchronization. Table 3–1 describes the attributes of this scheduled task. The procedure to configure scheduled tasks is described later in the guide.

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 were left empty, then reconciliation would not be performed.

Table 3–1 Attributes of the Lotus Notes Lookup Reconciliation Scheduled Task

Attribute	Description
ServerName	Enter the name of the IT resource instance that the connector must use to reconcile data. Default value: `LotusNotes`
LookupFieldName	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. The value can be either `Lookup.Lotus.Grp` or `Lookup.Lotus.OU`. Default value: `Lookup.Lotus.Grp`
Group/CertifierOU	Enter the name of the target system attribute from which values must be fetched. The value can be either `Group` or `CertifierOU`. Default value: `Group`

3.3 Configuring Reconciliation

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

- Section 3.3.1, "Full Reconciliation vs. Incremental Reconciliation"
- Section 3.3.2, "Limited Reconciliation"
- Section 3.3.3, "Batched Reconciliation"

- Section 3.3.4, "Reconciliation Scheduled Tasks"

3.3.1 Full Reconciliation vs. Incremental Reconciliation

When you run the Lotus Notes User Reconciliation scheduled task, only target system records that are added or modified after the last time the scheduled task was run are fetched into Oracle Identity Manager. This is incremental reconciliation.

You can perform a full reconciliation run to fetch all existing target system records into Oracle Identity Manager. To perform a full reconciliation run:

1. While performing the procedure described in Section 3.4, "Configuring Scheduled Tasks," enter the following values for the specified attributes of the scheduled task:

   - LastName: `nodata`
   - OU: `nodata`
   - Batch size: `All`
   - Certifier: `nodata`
   - Group: `nodata`

2. If you configure the connector for trusted source reconciliation, then set the value of the TrustedTimeStamp IT resource parameter to `None`. If you configure the connector for target resource reconciliation, then set the value of the NonTrustedTimeStampIT resource parameter to `None`.

   See Table 2–2 for information about these IT resource parameters.

After a full reconciliation run, the time stamp at which the reconciliation run ends is stored in the time stamp parameter of the IT resource. From the next reconciliation run onward, only target system records added or modified after the last reconciliation run are fetched to Oracle Identity Manager. In other words, incremental reconciliation is automatically activated from the next run onward.

3.3.2 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.

Creating a filter involves specifying a value for a target system attribute, which will be used in the query SELECT criteria to retrieve the records to be reconciled. You can specify values for any one or a combination of the following filter attributes, which are also target system attributes:

- LastName
- OU
- Group
- Certifier

If you want to use more than one target system attribute in the query criteria, then you must also specify the logical operator (AND or OR) that you want to apply to the combination of target system attributes that you select.

For example, suppose you specify the following values for these attributes:

- LastName: `Doe`
- OU: `DEL`
- Group: `All Access Group`
- Certifier: `OU=Telecom/O=Example`
- Operator: `OR`

Because you are using the `OR` operator, during reconciliation, only user records for which *any one* of these criteria is met are reconciled. If you were to use the `AND` operator, then the user records that are reconciled are the ones that meet both criteria.

While deploying the connector, follow the instructions in Section 3.4, "Configuring Scheduled Tasks" to specify values for these attributes and the logical operator that you want to apply.

3.3.3 Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- BatchSize: Use this attribute to specify the number of records that must be included in each batch. The default value is `1000`.
- NoOfBatches: Use this attribute to specify the total number of batches that must be reconciled. The default value is `All`.

If you specify a value other than `All`, then some of the newly added or modified user records may not get reconciled during the current reconciliation run. The following example illustrates this:

Suppose you specify the following values while configuring the scheduled tasks:

- BatchSize: `20`
- NoOfBatches: `10`

Suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 200 records would be reconciled during the current reconciliation run. The remaining 114 records would be reconciled during the next reconciliation run.

You specify values for the BatchSize and NoOfBatches attributes by following the instructions described in Section 3.3.4, "Reconciliation Scheduled Tasks."

3.3.4 Reconciliation Scheduled Tasks

You must specify values for the attributes of the following scheduled tasks:

> **Note:** See Section 3.4, "Configuring Scheduled Tasks" for the procedure.

- Section 3.3.4.1, "Scheduled Tasks for Reconciliation of User Records"

- Section 3.3.4.2, "Scheduled Task for Reconciliation of Deleted Users"

3.3.4.1 Scheduled Tasks for Reconciliation of User Records

Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled tasks:

- Lotus Notes User Reconciliation (scheduled task for target resource reconciliation)
- Lotus Notes Trusted User Reconciliation (scheduled task for trusted source reconciliation)

Table 3–2 describes the attributes of both scheduled tasks.

Table 3–2 Attributes of the Scheduled Tasks for Reconciliation of User Records

Attribute	Description	Default/Sample Value
TargetRO	Enter the name of the resource object.	`LOTUSRO` for target resource reconciliation `Xellerate User` for trusted source reconciliation
ServerName	Enter the name of the IT resource instance that the connector must use to reconcile data.	`LotusNotes`
IsTrusted	Specify whether the scheduled task must be used for trusted source reconciliation or target resource reconciliation.	For trusted source reconciliation, set the value of this attribute to `Yes`. For target resource reconciliation, set the value of this attribute to `No`.
LoginNameField	Specify the name of the OIM User form field whose value must be used as the login name for the OIM User. You must ensure that the field you select is unique for each IBM Lotus Notes and Domino user.	`Users.LastName` or `Users.ShortName`
XellerateOrganisation	Enter the default Oracle Identity Manager organization name that must be set for OIM Users created during trusted source reconciliation. **Note:** This attribute is used only during trusted source reconciliation.	`Xellerate Users`
BatchSize	Enter the number of records in each batch that must be fetched from the target system. This attribute is used during batched reconciliation. You must specify an integer value greater than zero. See Section 3.3.3, "Batched Reconciliation" for more information about this attribute.	The default value is `1000`.
NoOfBatches	Enter the number of batches to be reconciled. This attribute is used during batched reconciliation. The number of records in each batch is specified by the BatchSize attribute. See Section 3.3.3, "Batched Reconciliation" for more information.	Specify `All` if you want to reconcile all the batches. This is the default value. Specify an integer value greater than zero if you want to reconcile only a fixed number of batches.

Table 3–2 (Cont.) Attributes of the Scheduled Tasks for Reconciliation of User Records

Attribute	Description	Default/Sample Value
LastName	Enter the last name of the user whose records you want to reconcile. This attribute is used during limited reconciliation. If you do not want to use this filter attribute, then enter `nodata`. See Section 3.3.2, "Limited Reconciliation" for more information.	The value can be either the last name or `nodata`. The default value is `nodata`.
OU	Enter the OU of the users whose records you want to reconcile. This attribute is used during limited reconciliation. If you do not want to use this filter attribute, then enter `nodata`. See Section 3.3.2, "Limited Reconciliation" for more information.	The value can be either the OU of the users or `nodata`. The default value is `nodata`.
Certifier	Enter the name of the certifier for users whose records you want to reconcile. This attribute is used during limited reconciliation. If you do not want to use this filter attribute, then enter `nodata`. See Section 3.3.2, "Limited Reconciliation" for more information.	The value can be either the certifier of the users or `nodata`. The default value is `nodata`.
Group	Enter the name of the group for users whose records you want to reconcile. This attribute is used during limited reconciliation. If you do not want to use this filter attribute, then enter `nodata`. See Section 3.3.2, "Limited Reconciliation" for more information.	The value can be either the group of the users or `nodata`. The default value is `nodata`.
Operator	Enter the operator that you want to apply on the filter attributes. This attribute is used during limited reconciliation. See Section 3.3.2, "Limited Reconciliation" for more information.	The value can be `AND` or `OR`. The default value is `AND`.

3.3.4.2 Scheduled Task for Reconciliation of Deleted Users

Table 3–3 describes the attributes of the scheduled task for reconciliation of deleted users.

Table 3–3 Attributes of the Lotus Notes Delete User Reconciliation Task Scheduled Task

Attribute	Description
ServerName	Enter the name of the IT resource that the connector must use for reconciliation and provisioning operations. Default value: `Lotus Notes`

Table 3–3 (Cont.) Attributes of the Lotus Notes Delete User Reconciliation Task Scheduled Task

Attribute	Description
IsTrusted	Enter `No` if you want to configure the connector for target resource reconciliation. Enter `Yes` for trusted source reconciliation.
TargetRO	Enter `LOTUSRO` if you want to configure the connector for target resource reconciliation. Enter `Xellerate User` for trusted source reconciliation.
LoginNameField	Enter the attribute that you want to Parameter use as the login name for Xellerate User. Default value: `Users.LastName` **Note:** This attribute is used only if you configure the connector for trusted source reconciliation.

3.4 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–4 lists the scheduled tasks shipped as part of the connector.

Table 3–4 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
Lotus Notes Lookup Reconciliation	This scheduled task is used for lookup field synchronization.
Lotus Notes User Reconciliation	This scheduled task is used for user reconciliation in target resource mode.
Lotus Notes Trusted User Reconciliation	This scheduled task is used for user reconciliation in trusted source mode.
Lotus Notes Delete User Reconciliation Task	This scheduled task is used for reconciliation of deleted user records.

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Perform one of the following steps:
   a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
     b. In the search results table, click the edit icon in the Edit column for the scheduled task.
     c. On the Scheduled Task Details page where the details of the scheduled task that you selected 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 region, click **Search Scheduled Jobs**.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   Note:

   - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
   - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
   - Attributes of the scheduled task are discussed in Section 3.3.4, "Reconciliation Scheduled Tasks."

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

6. After specifying the attributes, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

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

   - 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.

3.5 Guidelines on Performing Provisioning

Apply the following guidelines while performing provisioning:

- You must enter values for the following mandatory attributes during provisioning operations:

  Last Name

  Server Name

  Password

- The IDFile Name and Mail File Name attributes are unique for each user. The Mail File Already Exists error message is displayed if you entering a file name that already exists on the target system.
- While performing a Create User provisioning operation, you *must* specify values for the following certifier-related fields on the process form, even though they are not marked as mandatory fields:

  Note: See Section 3.8, "Guidelines on Performing Reconciliation" for more information about these fields.

  – Certifier ID File Path: Enter the path to the ID file of the certifier on the target.

  – Certifier Password: Enter the password of the certifier corresponding to the ID file that you specify as the value of the Certifier ID File Path parameter.

  – Organization Unit: Specify the OU to which the user belongs.

Note: If an OU certifier is used, then the corresponding OU must be selected. However, if an organization certifier is used, then do *not* specify a value for the Organization Unit field.

- If you specify `True` as the value of the Create Mail DB File In Bckgrnd IT resource parameter, then the connector does not check whether mail files are successfully created during Create User provisioning operations.

3.6 Performing Provisioning Operations

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

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

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.7, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

This following are types of provisioning operations:

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

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

This section discusses the following topics:

- Section 3.6.1, "Direct Provisioning"
- Section 3.6.2, "Request-Based Provisioning"

3.6.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

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

   b. On the Create User page, enter values for the OIM User fields, and then click **Save**.

3. If you want to provision a target system account to an existing OIM User, then:

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

     a. From the Users menu, select **Manage**.

     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.

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

     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.

     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

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

   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:

     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.

     b. On the Resource Profile page, click **Provision New Resource**.

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

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

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

5. On the Step 1: Select a Resource page, select **LOTUSRO** 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 LOTUSRO 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 LOTUSRO Group Membership Details 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 Oracle Identity Manager release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.

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

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

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

3.6.2 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 3.6.2.1, "End User's Role in Request-Based Provisioning"
- Section 3.6.2.2, "Approver's Role in Request-Based Provisioning"

3.6.2.1 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 **LOTUSRO**, 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.

3.6.2.2 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.

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

Note: It is assumed that you have performed the procedure described in Section 2.3.1.6, "Enabling Request-Based Provisioning."

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

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

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

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

    c. Deselect the Auto Save Form check box.

    d. Click the Save icon.

3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **LOTUSRO** resource object.
   c. Deselect the Self Request Allowed check box.
   d. Click the Save icon.

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

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

3.8 Guidelines on Performing Reconciliation

Apply the following guidelines while performing provisioning:

- Values of the following fields are not fetched from the target system during reconciliation:
  - Certifier ID File Path
  - Certifier Password
  - Organization Unit

  When an account is created in Oracle Identity Manager through reconciliation of a new record from the target system, you must manually set values for these 3 fields. See Section 3.5, "Guidelines on Performing Provisioning" for information about setting values for these fields.

4 Extending the Functionality of the Connector

This chapter discusses the following optional procedures:

- Section 4.1, "Adding Standard Target System Attributes for Reconciliation"
- Section 4.2, "Adding Standard Target System Attributes for Provisioning"
- Section 4.3, "Configuring the Connector for Multiple Installations of the Target System"

4.1 Adding Standard Target System Attributes for Reconciliation

By default, the attributes listed in the "User Attributes for Target Resource Reconciliation and Provisioning" on page 1-6 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation as follows:

> **Note:** Perform this procedure only if you want to add new target system attributes for reconciliation. See *Oracle Identity Manager Design Console Guide* for detailed information about these steps.

1. Modify the attributemapping_recon.properties file, which is in the *OIM_HOME*/xellerate/XLIntegrations/LotusNotes/config directory.

   At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to add the attribute to the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

   ```
   OimAttributeName=TargetAttributeName
   ```

   For example:

   ```
   Users.City=City
   ```

   In this example, `City` is the reconciliation field and also the equivalent target system attribute. As a standard, the prefix "`Users.`" is added at the start of all reconciliation field names.

2. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:

   a. Open the Resource Objects form. This form is in the Resource Management folder.

   b. Click **Query for Records**.

c. On the Resource Objects Table tab, double-click the **LOTUSRO** resource object to open it for editing.

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

e. Specify a value for the field name.

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

   For example, if you uncomment the `Users.City=City` line in Step 1, then you must specify `Users.City` as the attribute name.

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

   For example: `String`

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

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

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

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

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

   b. Query for the **UD_LOTUS** form.

   c. Click **Create New Version.**

      The Create a New Version dialog box is displayed.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.2 Adding Standard Target System Attributes for Provisioning

> **Note:** In this section, the term "attribute" refers to the identity data fields that store user data.
>
> Do not repeat steps that you have performed as part of the procedure described in Section 4.1, "Adding Standard Target System Attributes for Reconciliation."

By default, the attributes listed in the "User Attributes for Target Resource Reconciliation and Provisioning" on page 1-6 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning as follows:

> **See Also:** *Oracle Identity Manager Design Console Guide*

1. Depending on the attribute that you want add for provisioning, modify the attributemapping_prov.properties file located in the *OIM_HOME*/xellerate/XLIntegrations/LotusNotes/config directory by performing one of the following steps:

> **Note:** A provisioning operation fails after you update the Alternate Full Name, Alternate Full Name Language, or Alternate Organizational Unit attributes. This has been documented as a known issue in Chapter 6, "Known Issues and Limitations."

- **For the Alternate Full Name attribute:**

  At the end of this file, add the following line:

  ```
  AlternateName=AlternateName,registerNewUser
  ```

  > **Note:** If you add the Alternate Full Name as an attribute for provisioning, then you must also add the Alternate Full Name Language attribute for provisioning.

- **For the Alternate Full Name Language attribute:**

  At the end of this file, add the following line:

  ```
  AlternateNameLanguage=AlternateNameLanguage,registerNewUser
  ```

  > **Note:** If you add the Alternate Full Name Language attribute, then you must also add the Alternate Full Name attribute for provisioning.

- **For the Alternate Organizational Unit attribute:**

  At the end of this file, add the following line:

  ```
  AlternateOrgUnit=AlternateOrgUnit,setAltOrgUnit,Vector
  ```

  Note: If you add the Alternate Organizational Unit attribute, then you must also add the Alternate Full Name and Alternate Full Name Language attributes for provisioning.

- **For attributes other than Alternate Full Name, Alternate Full Name Language, and Alternate Organizational Unit:**

  At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of provisioning attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

  ```
  OimAttributeName=TargetAttributeName
  ```

  For example:

  ```
  City=City
  ```

2. Add a new column in the process form.

   a. Open the Form Designer form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

   b. Query for the **UD_LOTUS** form.

   c. Click **Create New Version**.

      The Create a New Version dialog box is displayed.

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

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

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

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

   h. Specify the new field name and other values.

      If you added the Alternate Full Name Language attribute in Step 1, then ensure that you enter `LookupField` in the Field Type column. In addition, perform the following steps:

      – On the Properties tab, click the Field Name corresponding to Alternate Full Name Language attribute, and then click **Add Property.**

        The Edit Property dialog box is displayed.

      – From the **Property Name** list, select **Lookup Code.**

      – In the **Property Value** field, enter `Lookup.Lotus.Languages.`

      – Click the Save icon and close the Edit Property dialog box.

      – Add entries to the Lookup.Lotus.Languages lookup definition. You use the Lookup.Lotus.Languages lookup definition to specify a language for the user during a provisioning operation.

See Also: *Oracle Identity Manager Design Console* for instructions on adding entries to lookup definition

Entries in the Lookup.Lotus.Languages lookup definition must be in the following format:

Code Key	Decode
LANGUAGE_CODE	*LANGUAGE*

In this format, *LANGUAGE_CODE* is the code of a language on the target system, and *LANGUAGE* is the language.

Note: You must ensure that the languages for which you create entries in this lookup definition are enabled on the target system.

The following table lists sample values in the Lookup.Lotus.Languages lookup definition:

Code Key	Decode
en	English
fi	Finnish

3. Add a new variable in the variable list.

   a. Open the Adapter Factory form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

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

   c. On the Adapter Factory Table tab, double-click the **adpLNCreateuser** adapter from the list.

   d. On the Variable List tab, click **Add**.

   e. In the Add a Variable dialog box, specify the required values and then save and close the dialog box.

4. Define an additional adapter task for the newly added variable in the adpLNCreateuser adapter.

   a. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.

   b. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.

   c. In the Object Instance Selection dialog box, select **Persistent Instance** and then click **Continue**.

   d. In the Add an Adapter Factory Task dialog box, specify the task name, select the **setProperty** method from the **Method** list, and then click **Save**.

   e. Map the application method parameters, and then save and close the dialog box. To map the application method parameters:

   For the "Output: String Return variable (Adapter Variable)" parameter:

   i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select **Return variable**.

For the "Input: String (Adapter Variable)" parameter:

i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select **Input**.

For the "Input: String (Literal)" parameter:

i. From the **Map to** list, select **Literal**.

ii. From the **Name** list, select **String**.

iii. In the **Value** field, specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 1.

For example, if you uncomment the City=City line in Step 1, then you must specify City as the attribute name.

For the "Input: String (Adapter Variable)" parameter:

i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select the newly added adapter variable.

f. Repeat Steps a through e to create more adapter tasks.

5. Create an additional adapter task to set the input variable.

   a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.

   b. On the Adapter Tasks tab, click **Add**.

   c. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.

   d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.

6. Map the process form columns and adapter variables for the Create User process task as follows:

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

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

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

   d. On the Tasks tab, double-click the **Create User** task.

   e. In the Closing Form dialog box, click **Yes**.

   f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, and then save and close the dialog box. To map an unmapped variable:

      i. Double-click the row in which **N** is displayed in the Status column. The value `N` signifies that the variable is not mapped.

      ii. From the **Map to** list in the Edit Data Mapping for Variables dialog box, select **Process Data**.

      iii. From the **Qualifier** list, select the name of the variable.

7. If you want to enable updates of the attribute that you add for provisioning:

   Note:

   If you want to enable updates of the Alternate Name, Alternate Language, or Alternate Organizational Unit attributes, then ensure that you provision (create) a user with appropriate values for the Alternate Name and Alternate Language fields.

   The Alternate Full Name and Alternate Full Name Language attributes work in conjunction with each other. If you provide a value for one of these attributes, then you must also provide a value for the other attribute.

   Some of the steps in the following procedure are specific to the values that have been used. If you use other values, then these steps might need to be performed differently.

   a. Log in to the Oracle Identity Manager Design Console.

   b. Expand **Process Management** and then double-click **Process definition**.

   c. Enter `Lotus Process` in the **Name** field, and then click the **Query for records** button.

   d. In the process definition, add a new task for updating the field as follows:

      i. Click **Add** and enter the task name. For example, if you add the `City` field for provisioning, then add the `City Updated` task.

      ii. In the Task Properties section, ensure that the following fields only are selected:

      * Conditional

      * Disable Manual Insert

      * Allow Cancellation while Pending

      * Allow Multiple Instances

      iii. On the Task Dependency tab, under the Preceding Tasks section, click **Assign.**

      The Assign Preceding Tasks dialog box is displayed.

      iv. From the Existing Tasks section, select **Create User,** and the move it to the Preceding Tasks section by clicking the right arrow.

      v. Click **OK.**

   e. Click the **Integration** tab of the newly added task, and then click **Add**.

   f. Select **Adapter** as the handler type and then perform the following:

      a. If you are enabling updates on the Alternate Full Name, Alternate Full Name Language, or Alternate Organizational Unit fields, then select **LNUpdateUserName** and click **Save**.

      b. If you are enabling updates on fields other than Alternate Full Name, Alternate Full Name Language, or Alternate Organizational Unit, then select **LNUpdateUserInfo** and click **Save**.

c. In Adapter Variables, double click **attrName**. A window is displayed for editing the data mapping of the variable.

d. From the Map To list, select **Literal**.

e. Depending on the fields on which you are enabling updates, perform one of the following steps:

* If you are enabling updates on the Alternate Full Name, Alternate Full Name Language, or Alternate Organizational Unit fields, then in the Literal field, enter any value. For example, enter `AlternateFullName`.

* If you are enabling updates on fields other than Alternate Full Name, Alternate Full Name Language, or Alternate Organizational Unit, then in the Literal field, enter `City` as the name of the Oracle Identity Manager attribute. This value must be the same as that specified in the attributemapping_prov.properties file.

g. Create all required mappings.

h. Click the **Responses** tab of the task that you created in Step d. Add the SUCCESS and ERROR responses. Enter `C` for the SUCCESS response and `R` for the ERROR response.

If you are adding the Alternate Name, Alternate Language or Alternate Organizational Unit attribute as a UDF, then you must add the following response in addition to ones stated above:

Response: `ALT_FIELDS_ERROR`

Description: `Error in updating Alternate field.`

Status: `R`

i. Save the changes.

j. If you are enabling updates on the Alternate Full Name, Alternate Full Name Language, or Alternate Organizational Unit fields, then update the Lookup.Lotus.AltFieldMappings lookup definition.

See Also: *Oracle Identity Manager Design Console* for instructions on updating entries in a lookup definition

Depending on the field on which you are enabling updates, enter a Decode value for the corresponding Code Key. The Decode value must be the value that you entered in the Literal field in Step f.e. For example, if you are enabling updates on the Alternate Full Name field, then enter `AlternateFullName` as the Decode value for the AltFullName Code Key.

k. Save the changes.

4.3 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 IBM Lotus Notes and Domino.

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

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

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and scheduled task.

The decision to create a copy of a connector object is based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

To create copies of the connector objects:

> **Note:**
>
> For this connector, it is assumed that all installation of the target system have the same set of attributes for reconciliation and provisioning.
>
> See the *Oracle Identity Manager Design Console Guide* for detailed information about the steps in this procedure.

1. Create a copy of the IT resource. See "Configuring the IT Resource" on page 2-6 for information about this IT resource.
2. Create a copy of the Lotus Notes User Reconciliation scheduled task. See "Reconciliation Scheduled Tasks" on page 3-4 for information about this scheduled task.

To reconcile data from a particular target system installation, specify the name of the IT resource for that target system installation as the value of the ITResource scheduled task attribute.

5

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

- Section 5.1, "Testing the Connector"
- Section 5.2, "Troubleshooting"

5.1 Testing the Connector

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the testing utility:

1. Copy the files in the test/config directory on the installation media to the following directory:
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/XLIntegrations/LotusNotes/config
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/XLIntegrations/LotusNotes/config
2. Copy the files in the test/scripts directory on the installation media to the following directory:
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/XLIntegrations/LotusNotes/scripts
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/XLIntegrations/LotusNotes/scripts
3. Specify values for the parameters in the config.properties file. This file is in the config directory.

   See Also: Section 2.2.2, "Configuring the IT Resource" for information about the parameters in the config.properties file
4. Run one of the following scripts from the scripts directory:
   - For UNIX, run lotusNotes.sh.
   - For Microsoft Windows, run lotusNotes.bat.

5.2 Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the IBM Lotus Notes and Domino connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the IBM Lotus Notes and Domino server.	■ Ensure that the IBM Lotus Notes and Domino server is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record.
An Operation Failed message is displayed on the Oracle Identity Manager Administrative and User Console	■ Ensure that the attribute values do not contain delimiter characters (white space). ■ Ensure that the attribute values do not exceed the specified length.
The prompt for the password was aborted by user	The certifier account password specified as the value of the CertPwd IT resource parameter is not correct. Specify the correct password, and then try again.
Destination path does not exist	The directory path specified as the value of the IDFilePath IT resource parameter is not correct. Specify the correct path, and then try again.
Restricted operations not allowed in the server	The administrator whose user ID you have provided in the Admin IT resource parameter must belong to the Full Access Administrator list. Ensure that the administrator belongs to this list, and then try again.
Could not open the ID file	The path of the certifier ID file that you have specified as the value of the CertPath IT resource parameter is not correct. Specify the correct path, and then try again.
File does not exist (<username>)	The name of the mail template file specified as the value of the MailTemplateName IT resource parameter is not correct. Ensure that the mail template file exists on the target Domino server. This file is typically found in the data directory of the Domino server. Specify the correct mail template file name and then try again. For example, the name of the mail template file for IBM Lotus Notes and Domino Server version 6.*x* is mail6.ntf.
You are not authorized to perform that operation	The administrator whose user ID you have provided in the Admin IT resource parameter does not have the access privileges described in the "Enabling Modification of ID Files" section on page 2-21. Ensure that the administrator is assigned the required privileges, and then try again.
Suppose the following error message is displayed while provisioning in secure mode: NotesException: Could not get IOR from Domino Server.	Try using 63148 as the port number for the secure connection.

6 Known Issues and Limitations

The following sections describe known issues and limitations related to this release of the connector:

- Section 6.1, "Known Issues"
- Section 6.2, "Limitations"

6.1 Known Issues

There following is a known issue associated with this release of the connector:

- **Bug 7207232**

  Some Asian languages use multibyte character sets. If the character limit for fields on 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 point:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you have configured the target system for the Japanese language, then you would not be able to enter more than 25 characters in the same field.

- **Bug 11693279**

  A provisioning operation fails after you update the Alternate Full Name, Alternate Full Name Language, or Alternate Organizational Unit attributes.

- **Bug 16898634**

  Unable to create ID files for user accounts on shared drives.

  To workaround the issue, create a subdirectory in the UNC shared drive and ensure that the ID files are created in this subdirectory.

  For example, if you try to create ID files using the path \\<ServerName>\DominoShare, you might encounter the following error:

  The network name cannot be found.

  To create ID files, use the path \\<ServerName>\DominoShare\Test.

6.2 Limitations

The following is a connector limitation arising from a feature of the target system:

- On the target system, you can create an organizational policy to specify the encryption level that must be assigned to ID files generated when users are created. If you are using IBM Lotus Notes/Domino 6.5 or 7.*x*, then this encryption level is assigned to ID files generated during a Create User provisioning operation performed through Oracle Identity Manager. If you are using any other release of IBM Lotus Notes/Domino, then this encryption level is not assigned to the ID files. Instead, the default encryption level on the target system is assigned to the ID files.

Index