Oracle® Identity Manager

Connector Guide for IBM Lotus Notes and Domino

Release 9.0.4

E10428-07

July 2009

ORACLE®

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

E10428-07

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

Preface

This guide provides information about Oracle Identity Manager Connector for IBM Lotus Notes and Domino.

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at http://www.fcc.gov/cgb/consumerfacts/trs.html, and a list of phone numbers is available at http://www.fcc.gov/cgb/dro/trsphonebk.html.

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 9.0.4.7.

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 updates made from release 9.0.4 to the current release of the connector:

- 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 9.0.4.1.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" 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 "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-5 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 1-4, 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 3-4 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" 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 the following sections: ■ "Configuring the IT Resource" on page 2-7 ■ "Importing the Connector XML File" on page 2-11
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 3.

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.

Documentation-Specific Updates

The following sections discuss documentation-specific updates made from release 9.0.4 to the current release of the connector:

- 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 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" 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 Custom Attributes for Reconciliation" on page 3-6, 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" 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" 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" 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.

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with IBM Lotus Notes and Domino.

This chapter contains the following sections:

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

1.1 Reconciliation Module

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

See Also: The "Reconciliation" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

1.1.1 Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling group names from the target system to populate the lookup definition used for the Group Names lookup field on the process form.

1.1.2 User Reconciliation

User reconciliation involves reconciling the following fields:

1.1.2.1 Reconciled Resource Object Fields

The following target system fields are reconciled:

- FirstName
- MiddleName
- LastName
- ShortName
- OrgUnit
- MailInternetAddress
- Location
- Comment
- ForwardDomain
- SecurityType
- GrpName
- OldLastName
- OldFirstName
- OldMiddleName
- OldOrgUnit
- UniversalID
- ExpirationDate

1.1.2.2 Reconciled Xellerate User (OIM User) Fields

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

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

1.2 Provisioning Module

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

See Also: The "Provisioning" section in *Oracle Identity Manager Connector Concepts* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- FirstName
- MiddleName
- LastName
- ShortName
- Password
- OrgUnit
- MailInternetAddress
- Location
- Comment
- ForwardDomain
- EndDate
- SecurityType
- Grp
- ID File Name

1.3 Supported Functionality

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

Function	Type	Description
Add User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user
Update User Last Name	Provisioning	Updates the last name of a user
Update User First Name	Provisioning	Updates the first name of a user
Update User Middle Name	Provisioning	Updates the middle name of a user
Update User Organizational Unit	Provisioning	Updates the organizational unit of a user
Update User Short Name	Provisioning	Updates the short name of a user
Update User Mail Internet Address	Provisioning	Updates the e-mail address of a user
Update User Location	Provisioning	Updates the location of a user
Update User Comment	Provisioning	Updates the comment of a user
Update User Forward Domain	Provisioning	Updates the e-mail address to which e-mail for the user must be forwarded
Update User Password	Provisioning	Updates the user password and resets (or updates) the ID file
Disable User	Provisioning	Disables a user
Enable User	Provisioning	Enables a user
Reconcile lookup field	Reconciliation	Reconciles the lookup fields

Function	Type	Description
Reconcile User Data	Reconciliation	Trusted source reconciliation: Reconciles user data from IBM Lotus Notes and Domino to Oracle Identity Manager. A corresponding user is created in Oracle Identity Manager. If the user already exists in Oracle Identity Manager, then this user is updated. Target resource reconciliation: Reconciles user data from IBM Lotus Notes and Domino to Oracle Identity Manager. A user is not created in Oracle Identity Manager.

Note: The Delete User provisioning function is implemented by using the DeleteUser Administration Process (AdminP) function of IBM Lotus Notes and Domino. Similarly, the RenameNotesUser AdminP function is used to implement the following provisioning functions:

- Update User Last Name
- Update User First Name
- Update User Middle Name
- Update User Organizational Unit

1.4 Multilanguage Support

The connector supports the following languages:

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

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

1.5 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 1–1.

Table 1–1 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.
lib/xlLotusNotesProvision.jar	This JAR file contains the class files that are used to implement provisioning. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/JavaTasks
lib/xlLotusNotesRecon.jar	This JAR file contains the class files that are used to implement reconciliation. During connector deployment, this file is copied into the following directory: *OIM_HOME*/xellerate/ScheduleTask
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 into the following directory: *OIM_HOME*/xellerate/connectorResources **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
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.

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

File in the Installation Media Directory	Description
`test/config/config_unid.properties`	This file is used to store the value of the `UniqueID` user attribute while using the testing utility. See "Testing the Connector" on page 4-1 for more information about 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

1.6 Determining the Release Number of the Connector

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

Deploying the Connector

Deploying the connector involves the following steps:

- Verifying Deployment Requirements
- Using External Code Files
- Configuring the Target System
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
  - Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later
  - Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x
- Configuring Oracle Identity Manager
- Configuring SSL

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target systems	IBM Lotus Notes/Domino 6.5, 7.*x*, 8.0.*x*, 8.5

External code	`NCSO.jar`
	`Notes.jar`
	
	Refer to the "Copying the Connector Files" section on page 2-10 for more information about these files.

Target system user account	Domino Server administrator You must ensure that full administrative access has been assigned to this administrator account. In other words, this administrator must belong to the Full Access Administrator list. You provide the credentials of this user account while configuring the IT resource. The procedure is described later in this guide. If this user account is not assigned the specified privileges, then the following error message is displayed when Oracle Identity Manager tries to exchange data with the target system: `Invalid User Name`

2.2 Using External Code Files

Note: While installing Oracle Identity Manager in a clustered environment, 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_installation*`/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.

You must also copy the `NCSO.jar` and the `Notes.jar` files into the *OIM_HOME*`/xellerate/ThirdParty` directory before running the testing utility of the connector. The "Testing the Connector" section on page 4-1 describes the procedure to use the testing utility.

2.3 Configuring the Target System

Configuring the target system involves performing the following steps:

- Creating a Deny Access Group
- Enabling Modification of ID Files

2.3.1 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:
   - **Group name**: Specify a name for the group, for example, `noaccess`.
   - **Group type**: Select **Multi-purpose**.
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 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, you must:

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**.

2.3.2.1 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.

2.3.3 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.

2.4 Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later

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 on Oracle Identity Manager release 9.1.0 or later involves the following procedures:

- Running the Connector Installer
- Configuring the IT Resource

2.4.1 Running the Connector Installer

To run the Connector Installer:

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

   OIM_HOME/xellerate/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 *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then 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). If you want to import the target system as a trusted source for reconciliation, then see "Configuring the Target System As a Trusted Source" on page 3-2.

   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. Refer to "Clearing Content Related to Connector Resource Bundles from the Server Cache" on page 2-15 for information about running the `PurgeCache` utility.

   There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector

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

   c. Configuring the scheduled tasks that are created when you installed the connector

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

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 1–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, 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 1–1 for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.4.2 Configuring the IT Resource

Note: Perform this procedure if you are installing the connector on Oracle Identity Manager release 9.1.0 or later.

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. Expand **Resource Management.**
3. 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. The following table describes each parameter:

Parameter	Description
`AddBook`	Specifies whether or not the server entry in the Domino Directory is updated when the ID file is created The value can be `True` or `False`. The default value is `True`. 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`	User ID of the IBM Lotus Notes and Domino server administrator This administrator must belong to the Full Access Administrator list on IBM Lotus Notes and Domino.
`AdminPwd`	Password of the administrator

Parameter	Description
certifierOU	Specifies the OU of the certifier to be used when creating user accounts If you use a certifier on the target system, then you must specify the certifier OU value. If you do not have a certifier on the target system, then leave this parameter field empty. If there are multiple certifiers on the target system, then you must create one IT resource (of the Lotus Notes IT resource type) for each certifier. Refer to Oracle Identity Manager Design Console Guide for information about creating IT resources. If you specify a value for the certifierOU parameter, then the user OU value that you specify on the process form is ignored during the creation of a DN for a new user account. If you do not specify a value for the certifierOU parameter, then the user OU value that you specify on the process form is used in the DN. This feature ensures that only one OU value is included in the DN. If you specify a value for the certifierOU IT resource parameter, then user records for which the certifier OU value in the DN does not match the certifierOU parameter value are not reconciled. This is because the user DN is used to match records in the target system and Oracle Identity Manager, and a difference in the certifier OU value would lead to a mismatch in DN values. The following example illustrates this type of scenario: Suppose a user account on Lotus Notes has the following DN: CN=John Doe/OU=testcertou/O=test/C=US If testcertou has not been assigned as the value of the certifierOU parameter for any of the IT resources created on this Oracle Identity Manager installation, then the records of this user cannot be reconciled into Oracle Identity Manager. Sample value: NY
CertPath	Complete file specification of the certifier ID to be used when creating certifier ID files Sample value: C:\Lotus\Domino\Data\cert.id
CertPwd	Password of the certifier ID file
Create Mail ID File	Specifies whether or not a mail database is created with the ID file when calling the Register New User function of IBM Lotus Notes and Domino The value can be True or False. The default value is True.
Host	Host name or IP address of the IBM Lotus Notes and Domino server
Port	TCP/IP port at which the IBM Lotus Notes and Domino server is listening The default value is 63148.
IDFilePath	Path for storing the ID files
IDType	Type of ID files to be created The value can be HIERARCHICAL or CERTIFIER. The default is 172 (HIERARCHICAL). The numeric value for CERTIFIER is 173.
MailDBPath	Mail file path
MailOwnerAccess	Mail database ACL setting for the owner The value can be one of the following: ■ 0: MANAGER ■ 1: DESIGNER ■ 2: EDITOR The default value is 0.
MailQuotaLimit	Maximum size of the user's e-mail database, in megabytes The default value is 50.

Parameter	Description
MailQuotaWarning	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	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.
MailSystem	User's mail system The value can be any one of the following: ■ 0: NOTES ■ 3: INOTES ■ 4: INTERNET The default value is 0.
MailTemplateName	Name of the template for the mail file
PasswordLength	Minimum number of characters that can be used in the password The value can be any number. The default minimum length is 5 characters.
RegLog	Name of the log file to be used when creating IDs The default value is log.nsf.
RegServer	Name of the server to be used when creating IDs and performing other registration functions
StoreAddBook	Indicates whether or not the ID file is stored in the Domino Directory of the server The value can be True or False. The default value is True.
Sync Internet Password	Specifies whether or not the user can use the same password for both local client-based access and Web-based access to IBM Lotus Notes and Domino The value can be True or False. The default value is True.
IsSecure	Specifies whether or not the SSL feature is enabled The value can be Yes or No. The default value is Yes. **Note:** It is recommended that you enable SSL to secure communication with the target system.
DenyAccessGroupName	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 2-2.
triggerAdminp	Specifies whether or not the Trigger AdminP feature is enabled The value can be Yes or No. The default value is Yes.
isAgentInstalled	Specify Yes as the value of this parameter if you want to enable support for encrypted e-mail on the target system. Otherwise, specify No. **See Also:** The "Enabling Modification of ID Files" section on page 2-3 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 value at which the reconciliation run ends. The default value is None. Do not change it.

Parameter	Description
NonTrustedTimeStamp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is None. Do not change it.
Max Retries	Number of times that the Lotus Notes Connector should retry connecting to the target server if the connection fails The default value is 2.
Delay	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, in case the connection fails The default value is 10000.
TerminatedGroupName	Specifies 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 in the Domino Directory to be deleted before an administration process request is issued. ■ Enter No if you want to let the administration process make all required deletions.
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.

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

2.5 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.x

Installing the connector on any Oracle Identity Manager release between releases 8.5.3.1 and 9.0.3.x involves the following procedures:

- Copying the Connector Files
- Importing the Connector XML File

2.5.1 Copying the Connector Files

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

See Also: "Files and Directories on the Installation Media" section on page 1-4 for more information about these files

File in the Installation Media Directory	Destination Directory
Files in the config directory	*OIM_HOME*/xellerate/XLIntegrations/LotusNotes/config
lib/xlLotusNotesProvision.jar	*OIM_HOME*/xellerate/JavaTasks

File in the Installation Media Directory	Destination Directory
lib/xlLotusNotesRecon.jar	*OIM_HOME*/xellerate/ScheduleTask
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources
Files in the test/config directory	*OIM_HOME*/xellerate/XLIntegrations/LotusNotes/config
Files in the test/scripts directory	*OIM_HOME*/xellerate/XLIntegrations/LotusNotes/scripts
Files in the xml directory	*OIM_HOME*/xellerate/XLIntegrations/LotusNotes/xml

Note: In a clustered environment, copy the JAR files and the contents of the connectorResources directory to the corresponding directories on each node of the cluster.

2.5.2 Importing the Connector XML File

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the xlLotusNotesConnector.xml file, which is in the *OIM_HOME*/xellerate/XLIntegrations/LotusNotes/xml directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the LotusNotes IT resource is displayed.
8. Specify values for the parameters of the LotusNotes IT resource. Refer to the following table for information about the values to be specified:

Parameter	Description
AddBook	Specifies whether or not the server entry in the Domino Directory is updated when the ID file is created The value can be True or False. The default value is True. 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	User ID of the IBM Lotus Notes and Domino server administrator This administrator must belong to the Full Access Administrator list on IBM Lotus Notes and Domino.
AdminPwd	Password of the administrator

Parameter	Description
certifierOU	Specifies the OU of the certifier to be used when creating user accounts If you use a certifier on the target system, then you must specify the certifier OU value. If you do not have a certifier on the target system, then leave this parameter field empty. If there are multiple certifiers on the target system, then you must create one IT resource (of the Lotus Notes IT resource type) for each certifier. Refer to Oracle Identity Manager Design Console Guide for information about creating IT resources. If you specify a value for the certifierOU parameter, then the user OU value that you specify on the process form is ignored during the creation of a DN for a new user account. If you do not specify a value for the certifierOU parameter, then the user OU value that you specify on the process form is used in the DN. This feature ensures that only one OU value is included in the DN. If you specify a value for the certifierOU IT resource parameter, then user records for which the certifier OU value in the DN does not match the certifierOU parameter value are not reconciled. This is because the user DN is used to match records in the target system and Oracle Identity Manager, and a difference in the certifier OU value would lead to a mismatch in DN values. The following example illustrates this type of scenario: Suppose a user account on Lotus Notes has the following DN: CN=John Doe/OU=testcertou/O=test/C=US If testcertou has not been assigned as the value of the certifierOU parameter for any of the IT resources created on this Oracle Identity Manager installation, then the records of this user cannot be reconciled into Oracle Identity Manager. Sample value: NY
CertPath	Complete file specification of the certifier ID to be used when creating certifier ID files Sample value: C:\Lotus\Domino\Data\cert.id
CertPwd	Password of the certifier ID file
Create Mail ID File	Specifies whether or not a mail database is created with the ID file when calling the Register New User function of IBM Lotus Notes and Domino The value can be True or False. The default value is True.
Host	Host name or IP address of the IBM Lotus Notes and Domino server
Port	TCP/IP port at which the IBM Lotus Notes and Domino server is listening The default value is 63148.
IDFilePath	Path for storing the ID files
IDType	Type of ID files to be created The value can be HIERARCHICAL or CERTIFIER. The default is 172 (HIERARCHICAL). The numeric value for CERTIFIER is 173.
MailDBPath	Mail file path
MailOwnerAccess	Mail database ACL setting for the owner The value can be one of the following: ■ 0: MANAGER ■ 1: DESIGNER ■ 2: EDITOR The default value is 0.
MailQuotaLimit	Maximum size of the user's e-mail database, in megabytes The default value is 50.

Parameter	Description
MailQuotaWarning	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	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.
MailSystem	User's mail system The value can be any one of the following: ■ 0: NOTES ■ 3: INOTES ■ 4: INTERNET The default value is 0.
MailTemplateName	Name of the template for the mail file
PasswordLength	Minimum number of characters that can be used in the password The value can be any number. The default minimum length is 5 characters.
RegLog	Name of the log file to be used when creating IDs The default value is log.nsf.
RegServer	Name of the server to be used when creating IDs and performing other registration functions
StoreAddBook	Indicates whether or not the ID file is stored in the Domino Directory of the server The value can be True or False. The default value is True.
Sync Internet Password	Specifies whether or not the user can use the same password for both local client-based access and Web-based access to IBM Lotus Notes and Domino The value can be True or False. The default value is True.
IsSecure	Specifies whether or not the SSL feature is enabled The value can be Yes or No. The default value is Yes. Note: It is recommended that you enable SSL to secure communication with the target system.
DenyAccessGroupName	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 2-2.
triggerAdminp	Specifies whether or not the Trigger AdminP feature is enabled The value can be Yes or No. The default value is Yes.
isAgentInstalled	Specify Yes as the value of this parameter if you want to enable support for encrypted e-mail on the target system. Otherwise, specify No. **See Also:** The "Enabling Modification of ID Files" section on page 2-3 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 value at which the reconciliation run ends. The default value is None. Do not change it.

Parameter	Description
NonTrustedTimeStamp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is None. Do not change it.
Max Retries	Number of times that the Lotus Notes Connector should retry connecting to the target server if the connection fails The default value is 2.
Delay	Delay (in milliseconds) before the connector attempts to retry connecting to the target system, in case the connection fails The default value is 10000.
TerminatedGroupName	Specifies 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 in the Domino Directory to be deleted before an administration process request is issued. ■ Enter No if you want to let the administration process make all required deletions.
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.

Note: If there are multiple certifiers on the target system, then you must create one IT resource (of the Lotus Notes IT resource type) for each certifier. Refer to *Oracle Identity Manager Design Console Guide* for information about creating IT resources.

9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the Lotus Notes IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

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

11. Click **View Selections**.

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

2.6 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

Note: In a clustered environment, you must perform this step on each node of the cluster.

- Changing to the Required Input Locale
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

2.6.1 Changing to the Required Input Locale

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

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

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

While performing the instructions described in the "Copying the Connector Files" section on page 2-10, you copy files from the `resources` directory on the installation media into the *`OIM_HOME`*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the *`OIM_HOME`*`/xellerate/bin` directory.

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

   `OIM_HOME``\xellerate\bin\`*`batch_file_name`*

2. Enter one of the following commands:

   - 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.

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

OIM_HOME/xellerate/config/xlConfig.xml

2.6.3 Enabling Logging

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

- ALL

  This level enables logging for all events.

- DEBUG

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- OFF

  This level disables logging for all events.

The file in which you set the log level depends on the application server that you use:

- **Oracle WebLogic Server**

  To enable logging:

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

     log4j.logger.ADAPTER.LOTUSNOTES=log_level

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

     For example:

     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 line in the *OIM_HOME*/xellerate/config/log.properties file:

     log4j.logger.ADAPTER.LOTUSNOTES=log_level

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

   For example:

   ```
   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="ADAPTER.LOTUSNOTES">
        <priority value="log_level"/>
     </category>
     ```

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

     ```
     <category name="ADAPTER.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 line in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.ADAPTER.LOTUSNOTES=log_level
     ```

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

     For example:

     ```
     log4j.logger.ADAPTER.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

2.7 Configuring SSL

Note:

- This is an optional step of the deployment procedure. For more information about this procedure, refer to

  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 2-2, 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

Configuring the Connector

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

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

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Installations of the Target System

3.1 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:

- Partial Reconciliation
- Batched Reconciliation
- Configuring the Target System As a Trusted Source
- Configuring the Reconciliation Scheduled Tasks
- Adding Custom Attributes for Reconciliation

3.1.1 Partial 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

If you want to use both target system attributes to filter records, 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`
- 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 the "Specifying Values for the Scheduled Task Attributes" section on page 3-4 to specify values for these attributes and the logical operator that you want to apply.

3.1.2 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.
- `NumberOfBatches`: 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
- `NumberOfBatches`: 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 `NumberOfBatches` attributes by following the instructions described in the "Specifying Values for the Scheduled Task Attributes" section on page 3-4.

3.1.3 Configuring the Target System As a Trusted Source

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

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

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. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the `xlLotusNotes_XellerateUser.xml` file, which is in the *`OIM_HOME`*`/xellerate/XLIntegrations/LotusNotes/xml` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Importing the Connector XML File" section on page 2-11, the scheduled tasks for lookup fields, trusted source, and target resource reconciliation are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-4 for information about the values to be specified.

   See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
11. Repeat Steps 5 through 10 to configure the second scheduled task.

After you configure both scheduled tasks, proceed to the "Adding Custom Attributes for Reconciliation" section on page 3-6.

3.1.4.1 Specifying Values for the Scheduled Task Attributes

This section provides information about the values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Tasks

3.1.4.1.1 Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the `Lotus Notes Lookup Reconciliation` lookup fields reconciliation scheduled task.

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.

Attribute	Description	Default/Sample Value
`ServerName`	Name of the IT resource instance that the connector uses to reconcile data	`LotusNotes`
`LookupFieldName`	Name of the group lookup field that is to be reconciled	`LookUp.Lotus.Grp`

After you specify values for these task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

3.1.4.1.2 User Reconciliation Scheduled Tasks 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 trusted User Reconciliation` (Scheduled task for trusted source reconciliation)
- `Lotus Notes User Reconciliation` (Scheduled task for target resource reconciliation)

The following table describes the attributes of both scheduled tasks.

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.

Attribute	Description	Default/Sample Value
`TargetRO`	Name of the resource object	`LOTUSRO` for target resource reconciliation `Xellerate User` for trusted source reconciliation
`ServerName`	Name of the IT resource instance that the connector uses to reconcile data	`LotusNotes`
`IsTrusted`	Specifies whether or not reconciliation is to be carried out in trusted mode	For trusted source reconciliation, set the value of this attribute to `Yes`. For target resource reconciliation, set the value of this attribute to `No`.

Attribute	Description	Default/Sample Value
LoginNameField	Parameter whose value is used as the login name for the Xellerate User (OIM User) Ensure that the value of the parameter that you select is unique for each IBM Lotus Notes and Domino user.	Notes.LastName or Notes.ShortName
XellerateOrganisation	Default value for the Oracle Identity Manager Organization name This value is used to create the Xellerate User (OIM User) in trusted mode. **Note:** This attribute is specific to trusted source reconciliation.	Xellerate Users
BatchSize	Number of records in each batch that is reconciled You must specify an integer value greater than zero. **See Also:** The "Batched Reconciliation" section on page 3-2	The default value is 1000.
NoOfBatches	Number of batches to be reconciled The number of records in each batch is specified by the BatchSize attribute. **See Also:** The "Batched Reconciliation" section on page 3-2	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.
LastName	This is a filter attribute. Use this attribute to specify the last name of the user whose records you want to reconcile. If you do not want to use this filter attribute, then specify Nodata. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be either the last name or Nodata. The default value is Nodata.
OU	This is a filter attribute. Use this attribute to specify the OU of the users whose records you want to reconcile. If you do not want to use this filter attribute, then specify Nodata. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be either the OU of the users or Nodata. The default value is Nodata.
Operator	This is a filter attribute. Use this attribute to specify the operator that you want to apply on the filter attributes. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be AND or OR. The default value is AND.

After you specify values for these task attributes, proceed to Step 10 of the procedure to create scheduled tasks.

3.1.5 Adding Custom Attributes for Reconciliation

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

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

Note: You need not perform this procedure if you do not want to add custom attributes for reconciliation.

See Also: *Oracle Identity Manager Design Console* for detailed instructions on performing the following 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.

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.

3.2 Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

This section discusses the following topics related to configuring provisioning:

- Compiling Adapters
- Adding Custom Attributes for Provisioning

3.2.1 Compiling Adapters

Note: You must perform the procedure described in this section if you want to use the provisioning features of Oracle Identity Manager for this target system.

You need not perform the procedure to compile adapters if you have performed the procedure described in "Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later" on page 2-5.

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

> **See Also:** The "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector

- adpLNCreateuser
- adpLNUpdateUserName
- adpUpdateUserInfo
- adpLNDeleteUser
- adpLNEnableDisable
- adpLNUpdateGrp
- adpLNUpdatePassword
- LNPrepopulateLastName

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

To compile adapters by using the Adapter Manager form:

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

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

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

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM_HOME*/xellerate/Adapter directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

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

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

To view detailed information about an adapter:

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

3.2.2 Adding Custom Attributes for Provisioning

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

By default, the attributes listed in the "Provisioning Module" section on page 1-2 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. Modify the `attributemapping_prov.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 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.
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.

Repeat Steps 1 through 6 if you want to add more attributes.

Enabling Updates of the Field That You Add for Provisioning

To enable updates of the field that you add for provisioning:

> **Note:** 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.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Process Management** and then double-click **Process definition**.
3. Enter `Lotus Process` in the Name field, and then click the **Query for records** button.
4. Add a new task. For example, if you add the `City` field for provisioning, then add the `City Updated` task.
5. Click the **Integration** tab of the newly added task, and then click **Add**.
6. Select **Adapter** as the handler type and then perform the following:
   a. Select **LNUpdateUserInfo** and click **Save**.
   b. In Adapter Variables, double click **attrName**. A window is displayed for editing the data mapping of the variable.
   c. From the Map To list, select **Literal**.
   d. 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.
7. Create all required mappings.
8. Click the **Responses** tab of the `City Updated` task. Add the SUCCESS and ERROR responses. Enter `C` for the SUCCESS response and `R` for the ERROR response.
9. Save the changes.

3.3 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 may want to configure the connector for multiple installations of IBM Lotus Notes and Domino. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of IBM Lotus Notes and Domino.

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

See Also: *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

1. Create copies of the LotusNotes IT resource so that there is one IT resource for each installation of the target system.

   Refer to the "Importing the Connector XML File" section for information about the values to be specified for the IT resource parameters.

2. Create copies of the Lotus Notes trusted User Reconciliation, Lotus Notes User Reconciliation, and Lotus Notes Lookup Reconciliation scheduled tasks for each installation of the target system. While creating a scheduled task, specify attribute values corresponding to the target system installation for which you are creating the scheduled task.

   Refer to the "Specifying Values for the Scheduled Task Attributes" section for information about the values to be specified for the scheduled task attributes.

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the IBM Lotus Notes and Domino installation to which you want to provision the user.

4

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:

- Testing the Connector
- Troubleshooting

4.1 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 *`OIM_HOME`*`/xellerate/XLIntegrations/LotusNotes/config` directory.

   Copy the files in the `test/scripts` directory on the installation media to the *`OIM_HOME`*`/xellerate/XLIntegrations/LotusNotes/scripts` directory.

2. Specify values for the parameters in the `config.properties` file. This file is in the *`OIM_HOME`*`/xellerate/LotusNotes/config` directory.

   See Also: The "Importing the Connector XML File" section on page 2-11 for information about the parameters in the `config.properties` file

3. Run one of the following files:

   For UNIX:

   `OIM_HOME``/xellerate/XLIntegrations/LotusNotes/scripts/lotusNotes.sh`

   For Microsoft Windows

   `OIM_HOME``\xellerate\XLIntegrations\LotusNotes\scripts\lotusNotes.bat`

4.2 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 2-3. 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.

5

Known Issues

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

- **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.

- **Bug 8683657**

  Reconciliation events are not linked after updating the First Name or Last Name of a target system user record.

A

Attribute Mappings Between Oracle Identity Manager and IBM Lotus Notes and Domino

The following table lists attribute mappings between Oracle Identity Manager and IBM Lotus Notes and Domino:

Note: Apply the following guideline while performing provisioning operations:

Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you 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.

Oracle Identity Manager Attribute	IBM Lotus Notes and Domino Attribute	Description
First Name	FirstName	First name
Middle Name	MiddleName	Middle name
Last Name	LastName	Last name
Short Name	ShortName	Short name
Password	Password	Password
Security Type	SecurityType	Security type for user (North American or International)
End Date	ExpirationDate	Expiration date of certificate
Organizational Unit	OrgUnit	Organization to which user belongs
Mail Internet Address	InternetAddress	E-mail address.
Location	Location	Location
Comment	Comment	Comment
Forward Domain	ForwardDomain	Forwarding e-mail address
GRP Name	Group	Group to which user belongs

Oracle Identity Manager Attribute	IBM Lotus Notes and Domino Attribute	Description
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=LAST NAME/CN= FIRSTNAME MIDDLEINITIAL LASTNAME/OU=ORGANIZATIONUNIT/O=ORGANIZATION

Index

O

P

R

S

T

U

V

X