Oracle® Identity Manager

Connector Guide for IBM Lotus Notes and Domino

Release 9.0.3

B32354-02

March 2007

ORACLE®

Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino, Release 9.0.3

B32354-02

Contents

3 Testing and Troubleshooting

4 Known Issues

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

Index

Preface

Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino provides information about integrating Oracle Identity Manager with IBM Lotus Notes and Domino.

> **Note:** Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for IBM Lotus Notes and Domino.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. 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.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.3 connector documentation set, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

What's New in the Oracle Identity Manager Connector for IBM Lotus Notes and Domino?

This chapter provides an overview of the updates made to the connector and documentation for IBM Lotus Notes and Domino in release 9.0.3.1 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.3 release of this guide for information about updates that were new for the 9.0.3 release

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

  > **See Also:** *Oracle Identity Manager Release Notes*

Software Updates

This section discusses updates made to this release of the connector software.

Including a Certifier's OU in the DN Assigned to a New User Account

In this release, functionality related to including a certifier's OU in the DN assigned to a new user account has been modified. The following changes pertaining to this functionality update have been made in this guide:

- The "certifierOU IT Resource Parameter" section on page 2-9 discusses the functionality change.

- In the "Defining IT Resources" section on page 2-7, the `certifierOU` parameter has been added to the list of IT resource parameters.

Enabling Modification of ID Files

From this release onward, support for encrypted e-mail has been enhanced. The following changes pertaining to this functionality update has been made in this guide:

- The "Enabling Modification of ID Files" section on page 2-2 discusses this functionality change.

- In the "Defining IT Resources" section on page 2-7, the `isAgentInstalled` parameter has been added to the list of IT resource parameters.

New Error Messages Related to IT Resource Parameter Values

In the "Troubleshooting" section on page 3-2, a table providing solutions to errors related to IT resource parameter values has been added.

Documentation-Specific Updates

The following documentation-specific update has been made in this release of the guide:

- The "Creating a Deny Access Group" section on page 2-2 describes one of the procedures to be performed on the target system.

1

About the Connector

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

> **Note:** Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

- Supported Functionality
- Multilanguage Support
- Reconciliation Module
- Provisioning Module
- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector
- Converting Existing Date Values While Upgrading the Connector

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 Organization Unit	Provisioning	Updates the organization unit of a user
Update User Short Name	Provisioning	Updates the short name of a user

Function	Type	Description
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
Reconcile User Data	Reconciliation	Trusted mode: 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.
		Nontrusted mode: 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 Organization Unit

Multilanguage Support

This release of the connector supports the following languages:

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese

- Spanish

- Traditional Chinese

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

Reconciliation Module

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records.

Reconciliation can be divided into the following types:

- Lookup Fields Reconciliation
- User Reconciliation

Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the Group lookup field.

User Reconciliation

User reconciliation involves reconciling the following fields:

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

Provisioning Module

The following fields of IBM Lotus Notes and Domino are provisioned:

- FirstName
- MiddleName
- LastName

- ShortName

- Password

- OrgUnit

- MailInternetAddress

- Location

- Comment

- ForwardDomain

- EndDate

- SecurityType

- Grp

- ID File Name

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are compressed in the following directory on the installation media:

```
Collaboration and Messaging Applications\IBM Lotus Notes Domino
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
lib\JavaTask\xlLotusNotesProvision.jar	This JAR file contains the class files that are used to implement provisioning.
lib\ScheduleTask\xlLotusNotesRecon.jar	This JAR file contains the class files that are used to implement reconciliation.
Files in the resources directory	Each of these resource bundle files contains language-specific information that is used by the connector.
	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.
xml\xlLotusNotes_XellerateUser.xml	This XML file contains the configuration for the Xellerate 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
	■ Process form
	■ Process task and rule-generator adapters (along with their mappings)
	■ Resource object

The "Step 3: Copying the Connector Files and External Code" section on page 2-4 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

To determine the release number of the connector that you have deployed:

1. Extract the contents of the `xlLotusNotesRecon.jar` file. For a connector that has been deployed, this file is in the following directory:

    OIM_home`\xellerate\JavaTasks`

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.

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

Converting Existing Date Values While Upgrading the Connector

If you are upgrading from release 9.0.1 to release 9.0.2 of the connector and you want to migrate user data, then you must ensure that the migration scripts convert values stored in the `UD_LOTUS_ENDDATE` column from `VARCHAR2` to `DATE` format. In the earlier release, values were stored in the `DD/MM/YY` format as a string literal in this column.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Configuring the Target System
- Step 3: Copying the Connector Files and External Code
- Step 4: Configuring the Oracle Identity Manager Server
- Step 5: Importing the Connector XML File
- Step 6: Configuring Reconciliation
- Step 7: Compiling Adapters
- Step 8: Configuring SSL

If you want to configure the connector for multiple installations of IBM Lotus Notes and Domino, then perform the following procedure:

- Configuring the Connector for Multiple Installations of the Target System

Step 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 or later
Target systems	IBM Lotus Notes and Domino Server 6.5 or later

External code	`NCSO.jar`
	`Notes.jar`
	
	Refer to the "Step 3: Copying the Connector Files and External Code" section on page 2-4 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 performing the procedure in the "Defining IT Resources" section on page 2-7.

Step 2: Configuring the Target System

Configuring the target system involves performing the following steps:

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

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 performing the procedure described in the "Defining IT Resources" section on page 2-7, 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.

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 perform this step.

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 in the "Defining IT Resources" section on page 2-7.

To configure the agent on IBM Lotus Notes and Domino:

1. Log in to the Domino Admin client.

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

3. From the Server list in the Open Database dialog box, select the name of the Domino server.

4. In the **FileName** field, enter `names.nsf` and then click **Open**.

5. From the **View** menu, select **Agents**.

6. Click **New Agent**.

7. In 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. In 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 on 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. Click **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 Domino Admin client.

2. From the **File** menu, select **Database** and then select **Access Control**.

3. In the Access Control List dialog box, select **Manager** from the **Access** list and then select the **Delete documents** check box.

4. Click **OK**.

Additional Functionality Changes Related to the ID Files

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

- **ID File Name**

  In releases prior to the 9.0.3.1 release of the connector, when you create a user account through Oracle Identity Manager, the ID file name is created according to the following format:

  ```
  FirstNameLastName.id
  ```

  For example, if you create an account for user John Doe, then the ID file name is as follows:

  ```
  JohnDoe.id
  ```

  From the 9.0.3.1 release onward, you can now 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.

Ensuring That the Domino IIOP (DIIOP) Task Is Running

You must ensure that the Domino IIOP (DIIOP) task is running.

To do this, open the IBM Lotus Notes and Domino console and run the Load DIIOP command.

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

Step 3: Copying the Connector Files and External Code

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

> **Note:** The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:
>
> ```
> Collaboration and Messaging Applications\IBM Lotus Notes Domino
> ```
>
> Refer to the "Files and Directories That Comprise the Connector" section on page 1-4 for more information about these files.

File in the Installation Media Directory	Destination Directory
lib\JavaTask\xlLotusNotesProvision.jar	*OIM_home*\xellerate\JavaTasks
lib\ScheduleTask\xlLotusNotesRecon.jar	*OIM_home*\xellerate\ScheduleTask
Files in the resources directory	*OIM_home*\xellerate\connectorResources
Files in the xml directory	*OIM_home*\xlclient

After you copy the connector files, 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*\lotus\Domino 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.

> **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 connectorResources directory and all the JAR files mentioned in this section to the corresponding directories on each node of the cluster.

Step 4: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server 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

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.

To set the required input locale:

> **Note:** Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.

2. Double-click **Regional Options**.

3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the *OIM_home*\xellerate\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.

2. Enter one of the following commands:

   > **Note:** You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:
   >
   > *OIM_home*\xellerate\bin*batch_file_name*

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   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

   > **Note:** You can ignore the exception that is thrown when you perform Step 2.

Step 5: 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 locating files is displayed.

4. Locate and open the xlLotusNotesConnector.xml file, which is in the *OIM_home*\xlclient 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 table in the "Defining IT Resources" section on page 2-7 for information about the values to be specified.

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 Tools Reference Guide* for instructions.

11. Click **View Selections**.

    The contents of the XML file are displayed on the Import page. You may see a cross-shaped icon along with some nodes. Remove these nodes by right-clicking each node and then selecting **Remove.**

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

After you import the connector XML file, proceed to the

Defining IT Resources

You must specify values for the `LotusNotes` IT resource parameters listed in the following table.

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
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.
	See Also: The "certifierOU IT Resource Parameter" section on page 2-9 for more information about this parameter.
	Sample value: `certifierOU`
CertPath	Complete file specification of the certifier ID file to be used when creating user accounts
	Sample value: `C:\Lotus\Domino\Data\cert.id`
CertPwd	Password of the certifier

Parameter	Description
CreateMailIDFile	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.
IsDebug	Debug feature The value can be YES or NO. The default value is NO.
MailDBPath	Mail file path
MailOwnerAccess	Mail database ACL setting for the owner The value can be one of the following: ■ DESIGNER (1) ■ EDITOR (2) ■ MANAGER (0) The default value is 0.
MailQuotaLimit	Maximum size of the user's e-mail database, in megabytes The default value is 50.
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
MailSystem	User's mail system The value can be any one of the following: ■ INOTES (3) ■ INTERNET (4) ■ NOTES (0) The default value is 0.
MailTemplateName	Name of the template for the design of 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 use when creating IDs
RegServer	Name of the server to use when creating IDs and performing other registration functions

Parameter	Description
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.
SyncInternetPassword	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.
LastReconciliationTimeStamp	For the first reconciliation run, this parameter does not hold any value. From the second time onward, this parameter stores the time at which the last reconciliation run was completed.
	The default value is None.
IsSecure	Specifies whether or not the SSL feature is enabled
	The value can be YES or NO. The default value is NO.
	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 following 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 2-2 for more information about this parameter.

After you specify values for these IT resource parameters, proceed to Step 9 of the procedure to import connector XML files.

certifierOU IT Resource Parameter

In releases prior to the 9.0.3.1 release of this connector, the following problem is observed while creating a user account on the target system through Oracle Identity Manager:

Suppose you specify the following values while creating a user account directly on Lotus Notes:

- FirstName: John

- LastName: Doe

When the user account is created, a Distinguished Name (DN) similar to the following is assigned to the user:

CN=John Doe/OU=testcertou/O=test/C=US

In this sample DN, testcertou is the OU of the certifier for the user account that is created.

Suppose you specify the following values while creating a user account on Lotus Notes through Oracle Identity Manager:

- FirstName: `Jane`

- LastName: `Doe`

While creating the user account through Oracle Identity Manager, you can specify an OU for the user account on the process form. Suppose you specify `testuserou` as the user's OU on the process form. Then, a Distinguished Name (DN) similar to the following is assigned to the user:

`CN=Jane Doe/OU=testuserou/OU=testcertou/O=test/C=US`

This DN is invalid because it contains two OU attributes. If you try to search for and update this user, then the User Not Found error is thrown.

To resolve this problem, from the 9.0.3.1 release onward, the `certifierOU` parameter has been added to the Lotus Notes IT resource type. You use this parameter to specify the OU of a certifier on the target system.

> **Note:** If there are multiple certifiers on the target system, then you must create one IT resource (of the IT 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.

> **Caution:** 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.

Step 6: Configuring Reconciliation

Configuring reconciliation involves the following steps:

- Configuring Trusted Source Reconciliation

- Creating the Reconciliation Scheduled Tasks

Configuring Trusted Source Reconciliation

> **Note:** Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you import the `xlLotusNotes_XellerateUser.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.
>
> Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

To configure trusted source reconciliation, you must first import the XML file for trusted source reconciliation as follows:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.

3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.

4. Locate and open the `xlLotusNotes_XellerateUser.xml` file, which is in the `OIM_home\xlclient` 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**.

Then, set the value of the `IsTrusted` reconciliation scheduled task attribute to `YES` while performing the procedure described in the following section.

Creating the Reconciliation Scheduled Tasks

To create the scheduled tasks for lookup fields and user reconciliations:

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 ERROR 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 2-12 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 create the second scheduled task.

After you create both scheduled tasks, proceed to the "Step 7: Compiling Adapters" section on page 2-13.

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 Task

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the 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.

Attribute	Description	Default/Sample Value
TargetRO	Name of the resource object	LOTUSRO
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.

User Reconciliation Scheduled Task You must specify values for the following attributes of the user 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.

Attribute	Description	Default/Sample Value
TargetRO	Name of the resource object	LOTUSRO
ServerName	Name of the IT resource instance that the connector uses to reconcile data	LotusNotes
IsTrusted	Specifies whether or not reconciliation must be performed in trusted mode	YES or NO The default value is NO.
LoginNameField	Parameter whose value is used as the login name for the Xellerate 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
Notes.XellerateO rganisation	Default value for the Oracle Identity Manager Organization name This value is used to create the Xellerate User in trusted mode.	Xellerate Users

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

Step 7: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

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

You must compile these adapters before you can use them to provision accounts on the target system.

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.

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.

> **Note:** To compile one adapter at a time, use the Adapter Factory
> form. Refer to *Oracle Identity Manager Tools Reference Guide* for
> information about using the Adapter Factory and Adapter Manager
> forms.

Step 8: 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/

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
> "Step 2: 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 path of the data
   directory:

   lotus_home\Lotus\Domino\Data

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_installation*\jre\lib\ext directory on the Oracle Identity Manager server.

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. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

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

1. Create and configure one resource object per target system installation.

    The Resource Objects form is in the Resource Management folder. The `LOTUSRO` resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource per resource object.

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

3. Design one process form for each resource object.

    The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

    - `UD_LOTUS` (main form)
    - `UD_LNGRP` (child form)

    You can use these process forms as templates for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

    The Process Definition form is in the Process Management folder. The `Lotus Process` process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

    While creating process definitions for each target system installation, the following steps that you must perform are specific to the creation of each process definition:

    - From the **Object Name** lookup field, select the resource object that you create in Step 1.

    - From the **Table Name** lookup field, select the process form that you create in Step 3.

    - While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.

5. Configure reconciliation for each target system installation. Refer to the "Step 6: Configuring Reconciliation" section on page 2-10 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

   ■ `TargetRO`

   ■ `ServerName`

   ■ `IsTrusted`

   Set the `IsTrusted` attribute to `YES` for the IBM Lotus Notes and Domino installation that you want to designate as a trusted source. You can designate either a single or multiple installations of IBM Lotus Notes and Domino as the trusted source. For the remaining IBM Lotus Notes and Domino installations, set this attribute to `NO`.

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

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

3

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:

- Running Test Cases
- Troubleshooting

Running Test Cases

You can use the troubleshooting 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 troubleshooting utility, in a command window, change to the *OIM_home*\xellerate\JavaTasks directory, in which the xlLotusNotesProvision.jar file is present. Then, perform the following tests:

- Create an IBM Lotus Notes and Domino user as follows:

  ```
  java -jar xlLotusNotesProvision.jar Create host portNo admin  adminpassword \
  certpath regsrv  maildbpath reglog lastName  idpath  mailserver  firstName \
  password certpws mailtemplatename;
  ```

  For example:

  ```
  java -jar xlLotusNotesProvision.jar Create 172.21.106.106  63148 "John \
  Doe/TEST" password C:\\Test\\cert.id SGM mail\\ log.nsf lname C:\\Test\\ \
  CN=SGM/O=TEST fname password password mail6.ntf;
  ```

- Update information, such as the first name and last name, of an IBM Lotus Notes and Domino user as follows:

  ```
  java -jar xlLotusNotesProvision.jar UpdateUserInfo host portNo \
  admin adminpassword mailserver firstName lastName middleName orgUnit \
  attrName attrValue;
  ```

- Update information, such as the location and forward domain, of an IBM Lotus Notes and Domino user as follows:

  ```
  java -jar xlLotusNotesProvision.jar UpdateUserName host portNo admin \
  adminpassword mailServer certPath certPassword firstName lastName \
  middleName orgUnit attrName attrValue;
  ```

- Delete an IBM Lotus Notes and Domino user as follows:

  ```
  java -jar xlLotusNotesProvision.jar Delete host \
  portNo admin adminpassword mailserver firstName lastName middleName orgUnit \
  ```

```
regserver;
```

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 following table describes solutions to errors related to the IT resource parameter values.

Error Message	Solution
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.
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 2-2. Ensure that the administrator is assigned the required privileges, and then try again.

4

Known Issues

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

- For the Update User function, the simultaneous update of more than one of the following fields is not possible:
  - First Name
  - Last Name
  - Middle Name
  - Organization Unit

- 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.

- IBM Lotus Notes and Domino does not have a unique field for a user.

- Reconciliation of a user whose name (first name or last name) has been updated once works correctly. However, if the name (first name or last name) is updated again, then this second update is not reconciled during the next reconciliation run.

  The following example illustrates this limitation:

  Suppose a user's first name and last name were updated from `John` and `Doe` to `John1` and `Doe1`, respectively. This update is reconciled correctly. In the second update, the first name and last name are changed to `John2` and `Doe2`, respectively. This update is not reconciled because the old first name and old last name values stored in IBM Lotus Notes and Domino are still `John` and `Doe`.

- The limitation described in the preceding point is also applicable to user deletion after updates to the first name or last name in IBM Lotus Notes and Domino.

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

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

A

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

The following table discusses attribute mappings between Oracle Identity Manager and IBM Lotus Notes and Domino.

Oracle Identity Manager Attribute	IBM Lotus Notes and Domino Attribute	Description
Lookup Fields		
Lookup.Lotus.Grp	GROUP	Name of group profiles to which users can be attached
User Attributes		
First Name	First name	First name
Middle Name	Middle name	Middle name
Last Name	Last name	Last name
Short Name	Short name	Short name
Password	Password	Password
Security Type	Security type	Security type for user (North American or International)
End Date	Certificate expiration date	Expiration date of certificate
Organization Unit	Unique org unit	Organization to which user belongs
Mail Internet Address	Internet address	Email address.
Location	Location	Location
Comment	Comment	Comment
Forward Domain	Forwarding address	Forwarding e-mail address
GRP Name	Group	Group to which user belongs

Index