

# Oracle® Identity Manager

## Connector Guide for IBM Lotus Notes and Domino



Release 11.1.1

E20466-18

June 2020

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Oracle Identity Manager Connector Guide for IBM Lotus Notes and Domino, Release 11.1.1

E20466-18

Copyright © 2017, 2020, Oracle and/or its affiliates.

Primary Author: Gowri. G.R

Contributing Authors: Alankrita Prakash

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

|                             |    |
|-----------------------------|----|
| Audience                    | ix |
| Documentation Accessibility | ix |
| Related Documents           | ix |
| Conventions                 | ix |

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

---

|                                |      |
|--------------------------------|------|
| Software Updates               | xi   |
| Documentation-Specific Updates | xiii |

## 1 About the Connector

---

|         |   |      |
|---------|---|------|
| 1.1     | Certified Components  | 1-2  |
| 1.2     | Usage Recommendations   | 1-2  |
| 1.3     | Certified Languages   | 1-3  |
| 1.4     | Connector Architecture  | 1-3  |
| 1.5     | Features of the Connector   | 1-5  |
| 1.5.1   | Support for Both Target Resource and Trusted Source Reconciliation            | 1-5  |
| 1.5.2   | Support for Limited Reconciliation  | 1-5  |
| 1.5.3   | Support for Both Full and Incremental Reconciliation                          | 1-5  |
| 1.5.4   | Support for Adding Attributes for Reconciliation and Provisioning             | 1-6  |
| 1.6     | Lookup Definitions Used During Reconciliation and Provisioning                | 1-6  |
| 1.6.1   | Lookup Definitions Synchronized with the Target System                        | 1-6  |
| 1.6.2   | Other Lookup Definitions  | 1-6  |
| 1.7     | Connector Objects Used During Target Resource Provisioning and Reconciliation | 1-10 |
| 1.7.1   | User Attributes   | 1-11 |
| 1.7.2   | Provisioning Functions  | 1-13 |
| 1.7.3   | Reconciliation Rule for Target Resource Reconciliation                        | 1-14 |
| 1.7.3.1 | Target Resource Reconciliation Rule   | 1-15 |
| 1.7.3.2 | Viewing Target Resource Reconciliation Rules                                  | 1-15 |

|         |  |      |
|---------|--|------|
| 1.7.4   | Reconciliation Action Rules for Target Resource Reconciliation | 1-16 |
| 1.7.4.1 | Target Resource Reconciliation Action Rules                    | 1-16 |
| 1.7.4.2 | Viewing Target Resource Reconciliation Action Rules            | 1-17 |
| 1.8     | Connector Objects Used in the Trusted Source Mode              | 1-17 |
| 1.8.1   | User Attributes for Trusted Source Reconciliation              | 1-18 |
| 1.8.2   | Reconciliation Rule for Trusted Source Reconciliation          | 1-18 |
| 1.8.2.1 | Trusted Source Reconciliation Rule                             | 1-18 |
| 1.8.2.2 | Viewing Trusted Source Reconciliation Rule                     | 1-19 |
| 1.8.3   | Reconciliation Action Rules for Trusted Source Reconciliation  | 1-19 |
| 1.8.3.1 | Trusted Source Reconciliation Action Rules                     | 1-20 |
| 1.8.3.2 | Viewing Trusted Source Reconciliation Action Rules             | 1-20 |

## 2 Deploying the Connector

---

|         |   |      |
|---------|---|------|
| 2.1     | Preinstallation   | 2-1  |
| 2.1.1   | Understanding the Connector Deployment Architecture                           | 2-1  |
| 2.1.2   | Files and Directories on the Connector Installation Media                     | 2-3  |
| 2.1.3   | Using External Code Files   | 2-3  |
| 2.1.4   | Creating a Target System Account for Connector Operations                     | 2-4  |
| 2.2     | Installation  | 2-7  |
| 2.2.1   | Installing the Domino Identity Connector on the Connector Server              | 2-7  |
| 2.2.2   | Running the Connector Installer   | 2-8  |
| 2.2.3   | Configuring the IT Resource   | 2-11 |
| 2.2.3.1 | Parameters of the IT Resource   | 2-11 |
| 2.2.3.2 | Edit an Existing IT Resource Instance   | 2-13 |
| 2.2.3.3 | Create a New IT Resource  | 2-14 |
| 2.3     | Postinstallation  | 2-14 |
| 2.3.1   | Configuring Oracle Identity Manager 11.1.2 or Later                           | 2-15 |
| 2.3.1.1 | Creating and Activating a Sandbox   | 2-15 |
| 2.3.1.2 | Creating a New UI Form  | 2-15 |
| 2.3.1.3 | Creating an Application Instance  | 2-16 |
| 2.3.1.4 | Publishing a Sandbox  | 2-16 |
| 2.3.1.5 | Harvesting Entitlements and Sync Catalog                                      | 2-16 |
| 2.3.1.6 | Updating an Existing Application Instance with a New Form                     | 2-16 |
| 2.3.2   | Localizing Application Instance Form  | 2-17 |
| 2.3.3   | Enabling the Reset Password Option in Oracle Identity Manager 11.1.2 or Later | 2-18 |
| 2.3.4   | Configuring Oracle Identity Manager   | 2-19 |
| 2.3.4.1 | Setting Up the Lookup.Configuration.Domino Lookup Definition                  | 2-19 |
| 2.3.4.2 | Configuring Trusted Source Reconciliation                                     | 2-20 |
| 2.3.4.3 | Changing to the Required Input Locale   | 2-21 |

|         |   |      |
|---------|---|------|
| 2.3.4.4 | Clearing Connector Resource Bundles Content from the Server Cache | 2-21 |
| 2.3.4.5 | Enabling Logging in the Java Connector Server                     | 2-22 |
| 2.3.4.6 | Enabling Request-Based Provisioning                               | 2-22 |
| 2.3.4.7 | Enabling IT Resource Name Values in the Process Form              | 2-25 |
| 2.3.5   | Configuring the Target System                                     | 2-25 |
| 2.3.5.1 | Creating a Deny Access Group                                      | 2-26 |
| 2.3.5.2 | Disabling a User Account  | 2-26 |
| 2.3.6   | Creating the IT Resource for the Connector Server                 | 2-26 |
| 2.4     | Upgrading the Connector   | 2-33 |
| 2.5     | Defining a Connector  | 2-34 |

## 3 Using the Connector

---

|         |  |      |
|---------|--|------|
| 3.1     | Performing First-Time Reconciliation   | 3-1  |
| 3.2     | Scheduled Job for Lookup Field Synchronization                                 | 3-1  |
| 3.3     | Configuring Reconciliation   | 3-2  |
| 3.3.1   | Performing Full Reconciliation and Incremental Reconciliation                  | 3-2  |
| 3.3.2   | Performing Limited Reconciliation  | 3-3  |
| 3.3.3   | Reconciliation Scheduled Jobs  | 3-3  |
| 3.3.3.1 | Scheduled Jobs for Reconciliation of User Records                              | 3-3  |
| 3.3.3.2 | Scheduled Jobs for Reconciliation of Deleted Users                             | 3-4  |
| 3.4     | Scheduled Jobs for Lookup Field Synchronization and Reconciliation             | 3-5  |
| 3.5     | Configuring Scheduled Jobs   | 3-6  |
| 3.6     | Action Scripts   | 3-7  |
| 3.6.1   | Understanding Action Scripts   | 3-8  |
| 3.6.2   | Configuration Examples   | 3-9  |
| 3.6.3   | Accessing Variables from Script  | 3-16 |
| 3.6.4   | Configuring Action Scripts   | 3-16 |
| 3.7     | Configuring Provisioning in Oracle Identity Manager Release 11.1.2.x           | 3-17 |
| 3.8     | Guidelines for Performing Provisioning   | 3-18 |
| 3.9     | Performing Provisioning Operations on Oracle Identity Manager Release 11.1.1.x | 3-18 |
| 3.9.1   | Direct Provisioning  | 3-19 |
| 3.9.2   | Request-Based Provisioning   | 3-20 |
| 3.9.2.1 | End User's Role in Request-Based Provisioning                                  | 3-20 |
| 3.9.2.2 | Approver's Role in Request-Based Provisioning                                  | 3-21 |
| 3.10    | Switching Between Request-Based Provisioning and Direct Provisioning           | 3-21 |
| 3.10.1  | Switching From Request-Based Provisioning to Direct Provisioning               | 3-22 |
| 3.10.2  | Switching From Direct Provisioning to Request-Based Provisioning               | 3-22 |
| 3.11    | Guidelines for Performing Reconciliation                                       | 3-22 |

## 4 Extending the Functionality of the Connector

---

|       |   |     |
|-------|---|-----|
| 4.1   | Adding Target System Attributes for Reconciliation                        | 4-1 |
| 4.2   | Adding Target System Attributes for Provisioning                          | 4-3 |
| 4.3   | Configuring Validation and Transformation                                 | 4-5 |
| 4.3.1 | Configuring Validation for Provisioning                                   | 4-5 |
| 4.3.2 | Configuring Validation for Reconciliation                                 | 4-7 |
| 4.3.3 | Configuring Reconciliation Transformation                                 | 4-7 |
| 4.4   | Configuring the Connector for Multiple Installations of the Target System | 4-8 |
| 4.5   | Moving the User Name in the Name Hierarchy                                | 4-9 |
| 4.6   | Creating and Updating WebUsers  | 4-9 |
| 4.7   | Resetting the User Password in IDVault                                    | 4-9 |

## 5 Testing and Troubleshooting

---

|     |                       |     |
|-----|-----------------------|-----|
| 5.1 | Testing the Connector | 5-1 |
| 5.2 | Troubleshooting       | 5-4 |

## 6 Known Issues and Workarounds

---

|     |   |     |
|-----|---|-----|
| 6.1 | Lotus Resource not Shown in Self Service UI | 6-1 |
|-----|---|-----|

## Index

---

## Index

---

## List of Figures

---

|      |  |      |
|------|--|------|
| 1-1  | Connector Architecture   | 1-4  |
| 1-2  | Reconciliation Rule for Target Resource Reconciliation         | 1-16 |
| 1-3  | Reconciliation Action Rules for Target Resource Reconciliation | 1-17 |
| 1-4  | Reconciliation Rule for Trusted Source Reconciliation          | 1-19 |
| 1-5  | Reconciliation Action Rules for Trusted Source Reconciliation  | 1-21 |
| 2-1  | Connector Deployment Architecture                              | 2-2  |
| 2-2  | Adding User to the ACL   | 2-5  |
| 2-3  | Adding User to the Registration Log ACL                        | 2-6  |
| 2-4  | Adding User to the Administration Requests ACL                 | 2-7  |
| 2-5  | Connector Installation Success Screen                          | 2-10 |
| 2-6  | Step 1: Provide IT Resource Information                        | 2-27 |
| 2-7  | Step 2: Specify IT Resource Parameter Values                   | 2-27 |
| 2-8  | Step 3: Set Access Permission to IT Resource                   | 2-30 |
| 2-9  | Step 4: Verify IT Resource Details                             | 2-31 |
| 2-10 | Step 5: IT Resource Connection Result                          | 2-32 |
| 2-11 | Step 6: IT Resource Created                                    | 2-33 |
| 3-1  | Lookup Domino Configuration                                    | 3-10 |
| 3-2  | Creating Lookup  | 3-11 |
| 3-3  | Linking Lookup   | 3-12 |
| 3-4  | Linking Lookup   | 3-14 |
| 3-5  | Configuring Lookup   | 3-15 |

## List of Tables

---

|     |  |      |
|-----|--|------|
| 1-1 | Certified Components   | 1-2  |
| 1-2 | Other Lookup Definitions   | 1-7  |
| 1-3 | Process Form Fields Used for Target Provisioning and Reconciliation                        | 1-11 |
| 1-4 | Mapping Form Fields to User Attributes for Target Resource Provisioning and Reconciliation | 1-12 |
| 1-5 | Provisioning Functions   | 1-14 |
| 1-6 | Action Rules for Target Resource Reconciliation  | 1-16 |
| 1-7 | OIM User Fields Used for Trusted Source Reconciliation                                     | 1-18 |
| 1-8 | Mapping Form Fields to User Attributes for Trusted Source Reconciliation                   | 1-18 |
| 1-9 | Action Rules for Trusted Source Reconciliation   | 1-20 |
| 2-1 | Files and Directories On the Connector Installation Media                                  | 2-3  |
| 2-2 | IT Resource Parameters   | 2-11 |
| 2-3 | Entries in the Lookup.Configuration.Domino Lookup Definition                               | 2-20 |
| 2-4 | Parameters in the Properties File  | 2-23 |
| 2-5 | Parameters of the IT Resource for the Connector Server                                     | 2-28 |
| 3-1 | Attributes of the Domino Connector Lookup Reconciliation Scheduled Job                     | 3-2  |
| 3-2 | Attributes of the Scheduled Jobs for Reconciliation of User Records                        | 3-4  |
| 3-3 | Attributes of the Domino Connector Delete Reconciliation Scheduled Job                     | 3-4  |
| 3-4 | Attributes of the Domino Connector Trusted Delete Reconciliation Scheduled Job Attribute   | 3-5  |
| 3-5 | Scheduled Jobs for Lookup Field Synchronization and Reconciliation                         | 3-6  |
| 3-6 | Output by ICF-INTG   | 3-9  |
| 5-1 | IT Resource Parameters   | 5-3  |



# Preface

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

## Audience

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

## Documentation Accessibility

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

### Access to Oracle Support

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

## Related Documents

For information about installing and using Oracle Identity Manager, visit the following Oracle Help Center page:

[http://docs.oracle.com/cd/E52734\\_01/oim/index.html](http://docs.oracle.com/cd/E52734_01/oim/index.html)

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

[http://docs.oracle.com/cd/E22999\\_01/index.htm](http://docs.oracle.com/cd/E22999_01/index.htm)

## Conventions

The following text conventions are used in this document:

---

| Convention      | Meaning  |
|-----------------|--|
| <b>boldface</b> | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| <i>italic</i>   | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.                  |

---

| <b>Convention</b> | <b>Meaning</b>   |
|-------------------|--|
| 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 11.1.1.6.0.

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

- [Software Updates](#)

This section describes updates made to the connector software.

- [Documentation-Specific Updates](#)

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

## Software Updates

The following section discusses the software updates:

### Software Updates for Release 11.1.1.6.0

This release contains the following software updates:

- **Support for Domino CA Certificates**

From this release onwards, the Domino connector supports CA Certificates for provisioning and reconciliation operations. A new ITResource field and process from field has been introduced as CA Certifier. See [User Attributes](#) for more details.

 **Note:**

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

- **Support for Organization Hierarchy Changes**

From this release onwards, the Domino connector supports moving a user name in the name hierarchy. A new process form field moveCertifier has been introduced. See [Moving the User Name in the Name Hierarchy](#) for more details.

- **Support for Changing Password in IDVAULT**

From this release onwards, the Domino connector supports password change in IDVault. See [Resetting the User Password in IDVault](#) for more details.

- **Support for Tracing Capabilities in Domino Connector**

From this release onwards, the Domino connector logging has been enhanced to log each event. See [Enabling Logging in the Java Connector Server](#) for more details.

- **Support for Domino Connector to be Run on Linux Client**

From this release onwards, the Domino connector can be run on Linux server with Linux notes client. See [Deploying the Connector](#) for more details.

## Resolved Issues

The following table lists issues resolved in this release of the connector:

| Bug Number | Issue  | Resolution   |
|------------|--|--|
| 13685938   | Domino connector to be compiled RHEL 32 and 64-bit.                              | This issue has been resolved. The Domino connector can be run on Linux server with Linux notes client from this release. |
| 16667338   | Notes connector error when passing null  | This issue has been resolved. Notes connector can pass the value successfully now.                                       |
| 16249631   | Can not configure Lotus Notes to support multiple mail file templates            | This issue has been resolved. Lotus Notes can be configure to support multiple file templates now.                       |
| 14117120   | No tracing capabilities in ICF based DOMINO connector                            | This issue has been resolved. Tracing to Domino connector has been added now.  |
| 12541960   | Support for CA certificates  | This issue has been resolved. Support for Domino CA certificates has been added now.                                     |
| 13768796   | HTTP change password should not need the old password                            | This issue has been resolved. HTTPPassword can be updated successfully without OldPassword now.                          |
| 12531662   | Changing password in IDVAULT throws unsupported exception                        | This issue has been resolved. Password in IDVAULT can be changed successfully now.                                       |
| 15899873   | Entitlement, Account name and Account ID tagging for R2 compatibility            | This issue has been resolved.  |
| 13547403   | When last name is changed, the ORGA unit is dropped from new DOMINO username     | This issue has been resolved.  |
| 15979570   | Configuring Lotus scripts to run on Lotus Domino ICF connector 11.1.1.5          | This issue has been resolved.  |
| 14124067   | Creating roaming users using Domino connector should be configurable             | This issue has been resolved. Creating roaming users using Domino connector can be configured successfully now.          |
| 14026948   | OIM calls "PASSWORD UPDATED" task instead of "UD_LOTUS UPDATED" task             | This issue has been resolved.  |
| 13958212   | OW- REQUEST for Domino ADMINISTRATIONPROCESS API to update ALTFULLNAME attribute | This issue has been resolved.  |

| Bug Number | Issue  | Resolution   |
|------------|--|--|
| 13547375   | Lotus notes connector 11.1.1.5 does not support organization hierarchy changes | This issue has been resolved. Lotus notes connector supports organization hierarchy changes now. |

## Documentation-Specific Updates

The following section discusses the documentation-specific updates:

### Documentation-Specific Updates in Release 11.1.1.6.0

The following documentation-specific updates have been made in revision "18" of release 11.1.1.6.0:

- The "Oracle Identity Governance or Oracle Identity Manager" row of [Table 1-1](#) has been updated to include support for Oracle Identity Governance 12c (12.2.1.4.0).
- A Note has been added for the **userDatabaseName** parameter in [Table 2-2](#)
- An issue regarding account modification after running the target user reconciliation has been added to [Troubleshooting](#).

The following documentation-specific updates have been made in revision "17" of release 11.1.1.6.0:

Minor updates to the document structure have been made for better readability.

The following documentation-specific update has been made in revision "16" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of [Table 1-1](#) has been renamed as "Oracle Identity Governance or Oracle Identity Manager" and also updated for Oracle Identity Governance 12c (12.2.1.3.0) certification.

The following documentation-specific updates have been made in revision "15" of release 11.1.1.6.0:

- The "Target systems" and "External code" rows of [Table 1-1](#) have been modified.
- Oracle Identity Manager interface names have been corrected throughout the document.
- The name of the "Known Issues" chapter has been changed to "Known Issues and Workarounds." In addition, [Known Issues and Workarounds](#) has been restructured.

The following documentation-specific update has been made in revision "14" of release 11.1.1.6.0:

Section 2.3.4.5, "Enabling Logging" has been removed and replaced with [Enabling Logging in the Java Connector Server](#).

- The following documentation-specific updates have been made in revision "13" of release 11.1.1.6.0:
  - The "Connector Server" row has been added to [Table 1-1](#).
  - The "JDK" row of [Table 1-1](#) has been renamed to "Connector Server JDK".

- The following documentation-specific update has been made in revision "12" of release 11.1.1.6.0:  
A "Note" regarding trusted source IT resource has been added at the beginning of [Configuring the IT Resource](#).
- The following documentation-specific updates have been made in revision "11" of release 11.1.1.6.0:
  - The "Oracle Identity Manager" row of [Table 1-1](#) has been updated.
  - Information specific to Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) has been added to [Usage Recommendations](#).
- The following documentation-specific updates have been made in revision "10" of release 11.1.1.6.0:
  - A "Note" has been added at the beginning of [Extending the Functionality of the Connector](#).
  - Section 4.8, "Configuring Lotus Domino for CA Process" has been removed.
- The following documentation-specific updates have been made in revision "9" of release 11.1.1.6.0:
  - The descriptions for parameter "administrationServer" of [Table 2-2](#) and "MailFileAction" of [Table 5-1](#) have been modified.
  - [Creating and Updating WebUsers](#) has been added.
- The following documentation-specific update has been made in revision "8" of release 11.1.1.6.0:  
A "Note" has been added to Description of Values column of the Lookup.Domino.UM.ReconAttrMap row in [Table 1-2](#).
- The following documentation-specific update has been made in revision "7" of release 11.1.1.6.0:  
Information about limited reconciliation has been modified in [Performing Limited Reconciliation](#).
- The following documentation-specific updates have been made in revision "6" of release 11.1.1.6.0:
  - An issue related to certorg data has been added to [Troubleshooting](#).
  - The "Target systems" row in [Table 1-1](#) has been updated.
- The following documentation-specific update has been made in revision "5" of release 11.1.1.6.0:  
In [Files and Directories on the Connector Installation Media](#) bundle/ org.identityconnectors.domino-2.0.1.jar has been changed to org.identityconnectors.domino-2.0.2.jar.

# 1

## About the Connector

This chapter introduces the IBM Lotus Notes and Domino 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 (OIM) with external, identity-aware applications. This guide discusses the connector that enables you to use IBM Lotus Notes and Domino either as a managed (target) resource or as an authoritative (trusted) source of identity data for OIM.

 **Note:**

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

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

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

 **Note:**

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

This chapter contains the following sections:

- [Certified Components](#)
- [Usage Recommendations](#)
- [Certified Languages](#)
- [Connector Architecture](#)
- [Features of the Connector](#)
- [Lookup Definitions Used During Reconciliation and Provisioning](#)
- [Connector Objects Used During Target Resource Provisioning and Reconciliation](#)
- [Connector Objects Used in the Trusted Source Mode](#)

## 1.1 Certified Components

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

**Table 1-1 Certified Components**

| Item  | Requirement   |
|---|---|
| Oracle Identity Governance or Oracle Identity Manager | <p>You can use one of the following releases of Oracle Identity Governance or Oracle Identity Manager:</p> <ul style="list-style-type: none"> <li>• Oracle Identity Governance 12c (12.2.1.4.0)</li> <li>• Oracle Identity Governance 12c (12.2.1.3.0)</li> <li>• Oracle Identity Manager 11g Release 1 Patch Set 1 (11.1.1.5.4) and any later BP in this release track</li> <li>• Oracle Identity Manager 11g Release 2 (11.1.2.0.0) and any later BP in this release track</li> <li>• Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)</li> </ul> |
| Target systems  | <p>IBM Lotus Notes/Domino 8, 8.5, 8.5.x, 9.0, 9.0.1</p> <p><b>Note:</b> You must install IBM Lotus Notes on the same computer as the connector.</p>   |
| Connector Server                                      | 11.1.2.1.0  |
| Connector Server JDK                                  | For Oracle Identity Manager 11g Release 2 (11.1.2.0) and any later BP in this release track, use JDK 1.6 or later   |
| External code   | <p>Notes.jar</p> <p>See <a href="#">Using External Code Files</a> for more information about these files.</p>   |

## 1.2 Usage Recommendations

Deploy and use one of these connector versions on the basis of the Oracle Identity Manager and target system versions.

- Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:
  - If you are using an Oracle Identity Manager release 9.1.0.1 or later and earlier than Oracle Identity Manager 11g Release 1 (11.1.1.5.0), then use the 9.0.4.x version of this connector.
  - If you are using Oracle Identity Manager 11g Release 1 (11.1.1.5.0) or later, Oracle Identity Manager 11g Release 2 BP04 (11.1.2.0.4) or later, or Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0), then use the latest 11.1.1.x version of this connector.
- Depending on the target system that you are using, you must deploy and use one of the following connectors:
  - If you are using the following target systems, then use the 9.0.4.x version of this connector:
    - Oracle Enterprise Linux 5.2
    - Solaris 8
  - If you are using the following target systems, then use the latest 11.1.1.x version of this connector:



- \* Exadata V2, ExaLogic X2-2
- \* Oracle Enterprise Linux later than 5.2+x86 (32-bit) and x64 (64-bit)
- \* Solaris 11

## 1.3 Certified Languages

These are the languages that the connector supports.

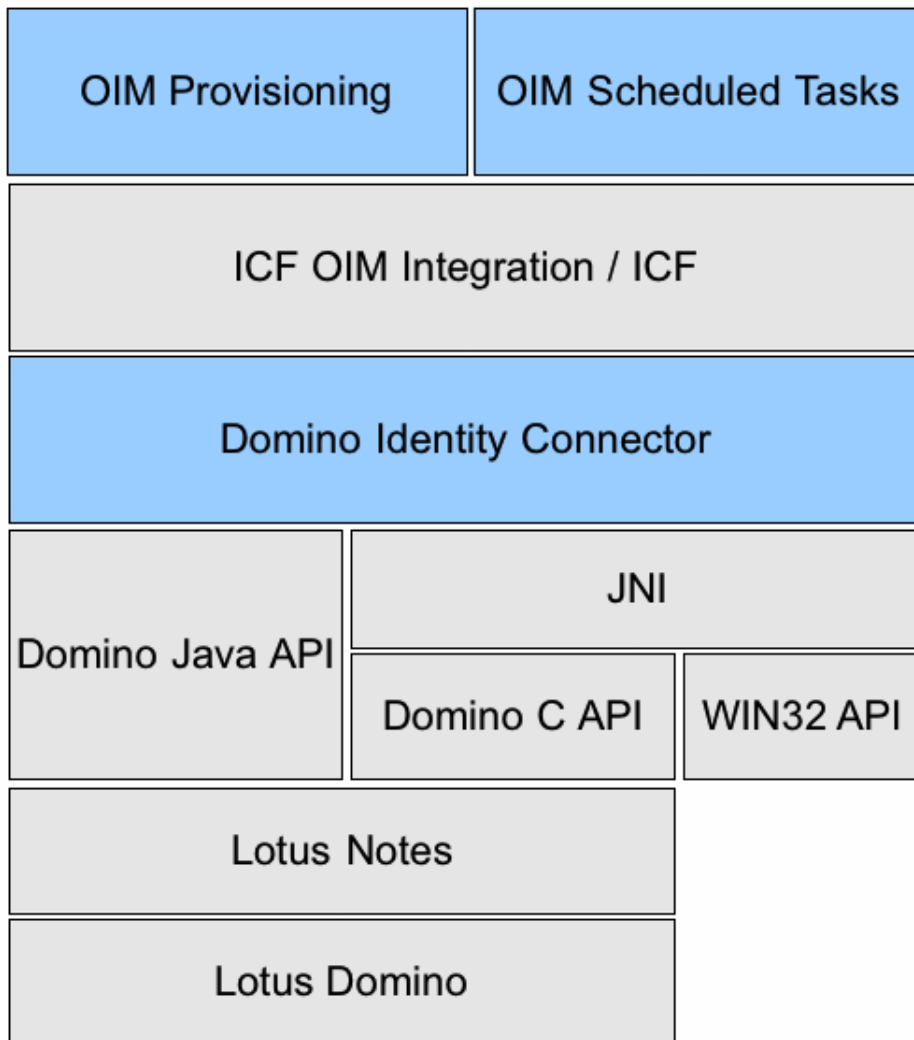
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

## 1.4 Connector Architecture

The Lotus Notes/Domino connector enables you to manage user accounts through Oracle Identity Manager.

[Figure 1-1](#) shows the architecture of the connector for IBM Lotus Notes and Domino.

Figure 1-1 Connector Architecture



You can configure the connector to run in one of the following modes:

- Identity Reconciliation
 

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

After an update, you must run trusted source reconciliation again so only that user is updated.
- Account Management
 

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

  - Provisioning

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

- Target resource reconciliation

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

 **Note:**

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

## 1.5 Features of the Connector

The features of the connector include full and incremental reconciliation, limited reconciliation, support for adding new attributes for reconciliation and provisioning and so on.

- [Support for Both Target Resource and Trusted Source Reconciliation](#)
- [Support for Limited Reconciliation](#)
- [Support for Both Full and Incremental Reconciliation](#)
- [Support for Adding Attributes for Reconciliation and Provisioning](#)

### 1.5.1 Support for Both Target Resource and Trusted Source Reconciliation

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

See [Configuring Reconciliation](#) for more information.

### 1.5.2 Support for Limited Reconciliation

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

See [Performing Limited Reconciliation](#) for more information.

### 1.5.3 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full

reconciliation run, change-based or incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time. See [Performing Full Reconciliation and Incremental Reconciliation](#) for more information.

## 1.5.4 Support for Adding Attributes for Reconciliation and Provisioning

You can add to the standard set of attributes for reconciliation and provisioning. [Extending the Functionality of the Connector](#) describes the procedure.

# 1.6 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during reconciliation and provisioning can be divided into the following categories:

- [Lookup Definitions Synchronized with the Target System](#)
- [Other Lookup Definitions](#)

## 1.6.1 Lookup Definitions Synchronized with the Target System

The Domino Connector Lookup Reconciliation scheduled job synchronizes the Lookup.Domino.Group lookup definition with the target system. The Lookup.Domino.Group lookup definition holds values for the Group lookup field on the process form.

Running this scheduled job populates the Lookup.Domino.Group lookup definition with group names fetched from the target system. For more information about the Domino Connector Lookup Reconciliation scheduled job, see [Scheduled Job for Lookup Field Synchronization](#).

## 1.6.2 Other Lookup Definitions

[Table 1-2](#) describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. Some of these lookup definitions are pre-populated with values. You must manually enter values for other definitions after the connector has been deployed.

In these Lookups, the Code Key column stores the process form field labels and the Decode column stores the Domino Attribute name.

**Table 1-2 Other Lookup Definitions**

| Lookup Definition                      | Description of Values   | Method to Specify Values for the Lookup Definition  |
|--|---|---|
| Combo.Domino.Security.Type             | <p>This definition holds information about security types that you can select for a target system account created through OIM.</p> <p>Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> 0 <b>DECODE:</b> International</li> <li>• <b>CODE:</b> 1 <b>DECODE:</b> North American</li> </ul> <p>These values are used in the License Type combo box. License Type determines which type of ID file is created, and affects encryption when sending or receiving mail and when encrypting data.</p>  | <p>This lookup definition is preconfigured. Do not add or modify entries in this lookup definition.</p>   |
| Lookup.Domino.UM.Configuration         | <p>This lookup definition holds information about the user attribute maps that you can select for a target system account created through OIM.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> Provisioning Attribute Map <b>DECODE:</b> Lookup.Domino.UM.ProvAttrMap</li> <li>• <b>CODE:</b> Recon Attribute Map <b>DECODE:</b> Lookup.Domino.UM.ReconAttrMap</li> </ul>   |   |
| Lookup.Domino.UM.Configuration.Trusted | <p>This lookup definition holds information about the trusted configuration for the Domino User object.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> Recon Attribute <b>DECODE:</b> Lookup.Domino.UM.TrustedDefaults</li> <li>• <b>CODE:</b> Recon Attribute Map <b>DECODE:</b> Lookup.Domino.UM.ReconAttrMap.Trusted</li> </ul>   |   |
| Lookup.Configuration.Domino            | <p>This lookup definition holds connector configuration entries that are used during reconciliation and provisioning.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> Bundle Name <b>DECODE:</b> org.identityconnectors.domino</li> <li>• <b>CODE:</b> Bundle Version <b>DECODE:</b> 2.0.1</li> <li>• <b>CODE:</b> Connector Name <b>DECODE:</b> org.identityconnectors.domino.DominoConnector</li> <li>• <b>CODE:</b> createIdFile <b>DECODE:</b> true</li> <li>• <b>CODE:</b> createMailDB <b>DECODE:</b> true</li> <li>• <b>CODE:</b> createMailDBInBackground <b>DECODE:</b> false</li> <li>• <b>CODE:</b> defaultPasswordExp <b>DECODE:</b> 720</li> <li>• <b>CODE:</b> formatUid <b>DECODE:</b> false</li> <li>• <b>CODE:</b> mailFileAction <b>DECODE:</b> 2</li> <li>• <b>CODE:</b> minPWLength <b>DECODE:</b> 5</li> <li>• <b>CODE:</b> northAmerican <b>DECODE:</b> false</li> <li>• <b>CODE:</b> storeIdInAddrBook <b>DECODE:</b> true</li> <li>• <b>CODE:</b> synclnetPassword <b>DECODE:</b> false</li> <li>• <b>CODE:</b> useIDVault <b>DECODE:</b> false</li> <li>• <b>CODE:</b> User Configuration Lookup <b>DECODE:</b> Lookup.Domino.UM.Configuration</li> </ul> <p>This lookup definition uses the User Configuration Lookup code key, which is an object type for a related lookup containing all information related to user type.</p> | <p>The entries in this lookup definition are preconfigured and should not require modification.</p> <p>To add entries, see <a href="#">Setting Up the Lookup.Configuration.Domino Lookup Definition</a> for instructions.</p> |

**Table 1-2 (Cont.) Other Lookup Definitions**

| Lookup Definition                   | Description of Values   | Method to Specify Values for the Lookup Definition  |
|-------------------------------------|---|---|
| Lookup.Domino.Notes Certifiers      | <p>This lookup definition holds information for the NotesCertifier object type.</p> <p>The Code Key and Decode value in this definition is:<br/> <b>CODE:</b> Shortname <b>DECODE:</b> ShortName</p> <p>You can configure Domino Connector Lookup Reconciliation to reconcile values into this lookup.</p>  |   |
| Lookup.Configuration.Domino.Trusted | <p>This lookup definition is the main configuration lookup for trusted reconciliation.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> Bundle Name <b>DECODE:</b> org.identityconnectors.domino</li> <li>• <b>CODE:</b> Bundle Version <b>DECODE:</b> 2.0.1</li> <li>• <b>CODE:</b> Connector Name <b>DECODE:</b> org.identityconnectors.domino.DominoConnector</li> <li>• <b>CODE:</b> createIdFile <b>DECODE:</b> true</li> <li>• <b>CODE:</b> createMailDB <b>DECODE:</b> true</li> <li>• <b>CODE:</b> createMailDBInBackground <b>DECODE:</b> false</li> <li>• <b>CODE:</b> defaultPasswordExp <b>DECODE:</b> 720</li> <li>• <b>CODE:</b> formatUid <b>DECODE:</b> false</li> <li>• <b>CODE:</b> mailFileAction <b>DECODE:</b> 2</li> <li>• <b>CODE:</b> minPWLength <b>DECODE:</b> 5</li> <li>• <b>CODE:</b> northAmerican <b>DECODE:</b> false</li> <li>• <b>CODE:</b> storeIdInAddrBook <b>DECODE:</b> true</li> <li>• <b>CODE:</b> synclnetPassword <b>DECODE:</b> false</li> <li>• <b>CODE:</b> useIDVault <b>DECODE:</b> false</li> <li>• <b>CODE:</b> User Configuration Lookup <b>DECODE:</b> Lookup.Domino.UM.Configuration.Trusted</li> </ul> <p>This lookup definition should be referenced in ITResource, and configured as Trusted ITResource.</p> | <p>The entries in this lookup definition are preconfigured and should not require modification.</p> |
| Lookup.Domino.UM.TrustedDefaults    | <p>This lookup definition holds mapping for all trusted reconciliation default values. These default values are used when a value is not received from the target resource.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> User Type <b>DECODE:</b> End-User</li> <li>• <b>CODE:</b> Employee Type <b>DECODE:</b> Full-Time</li> <li>• <b>CODE:</b> Organization <b>DECODE:</b> Xellerate Users</li> </ul>   |   |

**Table 1-2 (Cont.) Other Lookup Definitions**

| Lookup Definition                     | Description of Values  | Method to Specify Values for the Lookup Definition   |
|---------------------------------------|--|--|
| Lookup.Domino.UM.ReconAttrMap         | <p>This lookup definition holds mapping for all reconciliation operations between resource object fields and the target system attributes.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> Status <b>DECODE:</b> __ENABLE__</li> <li>• <b>CODE:</b> Mail File <b>DECODE:</b> MailFile</li> <li>• <b>CODE:</b> Universal Id <b>DECODE:</b> __UID__</li> <li>• <b>CODE:</b> Comment <b>DECODE:</b> Comment</li> <li>• <b>CODE:</b> Group List~Group [LOOKUP] <b>DECODE:</b> GroupList</li> </ul> <p><b>Note:</b> From this release onwards, GroupList is not a mandatory attribute for performing status reconciliation of a user. Hence, you can ignore or remove this attribute if you do not want to reconcile the groups of the user.</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> Mail Internet Address <b>DECODE:</b> InternetAddress</li> <li>• <b>CODE:</b> First Name <b>DECODE:</b> FirstName</li> <li>• <b>CODE:</b> Mail Server <b>DECODE:</b> MailServer</li> <li>• <b>CODE:</b> Mail Quota Limit <b>DECODE:</b> MailQuotaSizeLimit</li> <li>• <b>CODE:</b> Short Name <b>DECODE:</b> ShortName</li> <li>• <b>CODE:</b> Location <b>DECODE:</b> Location</li> <li>• <b>CODE:</b> Forwarding Domain <b>DECODE:</b> forwardingAddress</li> <li>• <b>CODE:</b> Organization Unit <b>DECODE:</b> OrgUnit</li> <li>• <b>CODE:</b> Middle Name <b>DECODE:</b> MiddleInitial</li> <li>• <b>CODE:</b> Mail Quota Warning <b>DECODE:</b> MailQuotaWarningThreshold</li> <li>• <b>CODE:</b> Last Name <b>DECODE:</b> LastName</li> </ul> | <p>This lookup definition is preconfigured.</p> <p><a href="#">Table 1-3</a> describes the default entries in this lookup definition.</p> <p>You can add entries to this lookup definition if you want to map new target system attributes for reconciliation. For more information, see <a href="#">Adding Target System Attributes for Reconciliation</a>.</p> |
| Lookup.Domino.UM.ReconAttrMap.Trusted | <p>This lookup definition holds mapping for all trusted reconciliation attributes.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> Status[TRUSTED] <b>DECODE:</b> __ENABLE__</li> <li>• <b>CODE:</b> User Login <b>DECODE:</b> ShortName</li> <li>• <b>CODE:</b> First Name <b>DECODE:</b> FirstName</li> <li>• <b>CODE:</b> Email <b>DECODE:</b> InternetAddress</li> <li>• <b>CODE:</b> Middle Name <b>DECODE:</b> MiddleInitial</li> <li>• <b>CODE:</b> Last Name <b>DECODE:</b> LastName</li> </ul>  | <p>This lookup definition is preconfigured.</p> <p><a href="#">Table 1-3</a> describes the default entries in this lookup definition.</p> <p>You can add entries to this lookup definition if you want to map new target system attributes for reconciliation. For more information, see <a href="#">Adding Target System Attributes for Reconciliation</a>.</p> |

Table 1-2 (Cont.) Other Lookup Definitions

| Lookup Definition                | Description of Values  | Method to Specify Values for the Lookup Definition  |
|----------------------------------|--|---|
| Lookup.Domino.UM.Pr<br>ovAttrMap | <p>This lookup definition holds mapping for all provisioning operations between resource object fields and target system attributes.</p> <p>The Code Key and Decode values in this definition are:</p> <ul style="list-style-type: none"> <li>• <b>CODE:</b> License Type <b>DECODE:</b> NorthAmerican</li> <li>• <b>CODE:</b> Last Name <b>DECODE:</b> LastName</li> <li>• <b>CODE:</b> Old Password <b>DECODE:</b> <code>__CURRENT_PASSWORD__</code></li> <li>• <b>CODE:</b> Certifier Password <b>DECODE:</b> credentials</li> <li>• <b>CODE:</b> Middle Name <b>DECODE:</b> MiddleInitial</li> <li>• <b>CODE:</b> Short Name <b>DECODE:</b> ShortName</li> <li>• <b>CODE:</b> End Date[DATE] <b>DECODE:</b> EndDate</li> <li>• <b>CODE:</b> Mail File Name <b>DECODE:</b> MailFile</li> <li>• <b>CODE:</b> Mail Server <b>DECODE:</b> MailServer</li> <li>• <b>CODE:</b> UD_LNGRP~Group Name[LOOKUP] <b>DECODE:</b> GroupList</li> <li>• <b>CODE:</b> Certifier Org Hierarchy[LOOKUP] <b>DECODE:</b> CertifierOrgHierarchy</li> <li>• <b>CODE:</b> Mail Quota Limit <b>DECODE:</b> MailQuotaSizeLimit</li> <li>• <b>CODE:</b> Recertify <b>DECODE:</b> Recertify</li> <li>• <b>CODE:</b> IDFile Name[PROVIDEONPSWDCHANGE] <b>DECODE:</b> idFile</li> <li>• <b>CODE:</b> Certifier ID File Path <b>DECODE:</b> certifierIDFile</li> <li>• <b>CODE:</b> Comment <b>DECODE:</b> Comment</li> <li>• <b>CODE:</b> Password <b>DECODE:</b> <code>__PASSWORD__</code></li> <li>• <b>CODE:</b> Mail Replica Servers <b>DECODE:</b> MailReplicaServers</li> <li>• <b>CODE:</b> Location <b>DECODE:</b> Location</li> <li>• <b>CODE:</b> Mail Quota Warning <b>DECODE:</b> MailQuotaWarningThreshold</li> <li>• <b>CODE:</b> Organization Unit <b>DECODE:</b> OrgUnit</li> <li>• <b>CODE:</b> Forward Domain <b>DECODE:</b> forwardingAddress</li> <li>• <b>CODE:</b> First Name <b>DECODE:</b> FirstName</li> <li>• <b>CODE:</b> Universal Id <b>DECODE:</b> <code>__UID__</code></li> <li>• <b>CODE:</b> Full Name <b>DECODE:</b> <code>__NAME__="{\${First_Name} \${Middle_Name} \${Last_Name}\${Certifier_Org_Hierarchy}"</code></li> <li>• <b>CODE:</b> Mail Internet Address <b>DECODE:</b> InternetAddress</li> </ul> | <p>This lookup definition is preconfigured. <a href="#">Table 1-3</a> lists the default entries in this lookup definition.</p> <p>You can add entries to this lookup definition if you want to map new target system attributes for provisioning. For more information, see <a href="#">Adding Target System Attributes for Provisioning</a>.</p> |

## 1.7 Connector Objects Used During Target Resource Provisioning and Reconciliation

This section describes the different connector objects that you use for target provisioning and reconciliation.

This information is organized into the following topics:

- [User Attributes](#)
- [Provisioning Functions](#)



- [Reconciliation Rule for Target Resource Reconciliation](#)
- [Reconciliation Action Rules for Target Resource Reconciliation](#)

## 1.7.1 User Attributes

The Process Form contains fields for Domino attributes that are supported "out-of-the-box." You must map these process form fields to Lotus Notes/Domino attributes for both provisioning and reconciliation, as follows:

- For provisioning, map the form fields to attributes in Lookup.Domino.UM.ProvAttrMap
- For reconciliation, map the form fields to attributes in Lookup.Domino.UM.ReconAttrMap

In these Lookups, the Code Key column stores the process form field labels and the Decode column stores the Domino Attribute name.

[Table 1-3](#) describes the form fields used for target resource provisioning and reconciliation.

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

| Process Form Field Label | Field Type    | Description   |
|--------------------------|---------------|---|
| Certifier ID File Path   | TextField     | Fully qualified path to the Certifier ID file   |
| Certifier Org Hierarchy  | LookupField   | Canonical or abbreviated name of the certifier. For example, if the certifier is: <ul style="list-style-type: none"> <li>• The organization certifier for the ACME organization, then the value should be /ACME</li> <li>• The organization unit, then the value should be similar to, /SomOU/ACME</li> </ul> This value is provided in the Lookup.Domino.NotesCertifiers lookup. You can configure this lookup to reconcile values from a target resource by using the Domino Connector Lookup Reconciliation task. You must provide this value to ensure correct functionality. |
| Certifier Password       | PasswordField | Password for the specified Certifier ID file  |
| Comment                  | TextField     | Comment   |
| End Date                 | DateFieldDlg  | End date  |
| First Name               | TextField     | First name  |
| Forwarding Domain        | TextField     | Forwarding e-mail address   |
| Last Name                | TextField     | Last name   |
| License Type             | ComboBox      | Type of ID file used to encrypt incoming or outgoing email and to encrypt data  |
| Location                 | TextField     | Location  |
| Mail File Name           | TextField     | Mail file name<br><b>Note:</b> A mail file is created only when you register a new user. Although, you can change the name in OIM, the file will not be renamed.  |
| Mail Internet Address    | TextField     | E-mail address  |

**Table 1-3 (Cont.) Process Form Fields Used for Target Provisioning and Reconciliation**

| Process Form Field Label | Field Type  | Description  |
|--------------------------|---|--|
| Mail Quota Limit         | TextField   | Maximum amount of emails permitted                     |
| Mail Quota Warning       | TextField   | Amount of mail is about to exceed or exceeds threshold |
| Mail Replica Servers     | TextField   | List of replica mail servers                           |
| Mail Server              | TextField   | Default mail server to use when creating users         |
| Middle Name              | TextField   | Middle name  |
| Organization Unit        | TextField   | Organization to which user belongs                     |
| Password                 | PasswordField   | Password   |
| Recertify                | CheckBox  | Recertify  |
| Server Name              | ITResourceLo  | Server name  |
| Short Name               | TextField   | Short name   |
| Universal Id             | DOField   | Universal ID   |
| CA Certifier             | Mention the hierarchical CA Certifier name here.<br>Example: /ca/org1<br>In this example, CA is the CA Certifier under org1 organization.                     | CA Certifier   |
| RoamSubDir               | roamingsub directory name.<br>Example: roaming<br>\roamuser   | RoamSubDir   |
| MoveCertifer             | If you check this check box moving a user name in the name hierarchy.<br>See <a href="#">Moving the User Name in the Name Hierarchy</a> for more information. | MoveCertifer   |

[Table 1-4](#) describes the mapping between the form fields and user attributes for target resource provisioning and reconciliation.

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

| Process Form Field              | IBM Lotus Notes and Domino Attribute |
|---------------------------------|--------------------------------------|
| Certifier ID File Path          | certifierIDFile                      |
| Certifier Org Hierarchy[LOOKUP] | CertifierOrgHierarchy                |
| Certifier Password              | credentials                          |
| Comment                         | Comment                              |
| End Date                        | GroupList                            |
| First Name                      | FirstName                            |

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

| Process Form Field                                      | IBM Lotus Notes and Domino Attribute   |
|---|--|
| Forward Domain ( <i>for provisioning</i> )              | forwardingAddress  |
| Forwarding Domain ( <i>for reconciliation</i> )         |  |
| Full Name   | __NAME__="{\${First_Name} \${Middle_Name}\${Last_Name}\${Certifier_Org_Hierarchy}" |
| Group List~Group[LOOKUP] ( <i>for reconciliation</i> )  | GroupList  |
| UD_LNGRP~Group Name[LOOKUP] ( <i>for provisioning</i> ) |  |
| IDFile Name[PROVIDEONPSWDCHANGE]                        | idFile   |
| Last Name   | LastName   |
| License Type  | NorthAmerican  |
| Location  | Location   |
| Mail File ( <i>for reconciliation</i> )                 | MailFile   |
| Mail File Name ( <i>for provisioning</i> )              | MailFile   |
| Mail Internet Address                                   | InternetAddress  |
| Mail Quota Limit  | MailQuotaSizeLimit   |
| Mail Quota Warning                                      | MailQuotaWarningThreshold  |
| Mail Replica Servers                                    | MailReplicaServers   |
| Mail Server   | MailServer   |
| Middle Name   | MiddleInitial  |
| Old Password  | _CURRENT_PASSWORD_   |
| Organization Unit                                       | OrgUnit  |
| Password  | _PASSWORD_   |
| Recertify   | Recertify  |
| Short Name  | ShortName  |
| Status ( <i>for reconciliation</i> )                    | _Enable_   |
| Universal Id  | _UID_  |

## 1.7.2 Provisioning Functions

Provisioning functions are basically provisioning process tasks that use adapters to perform provisioning operations.

[Table 1-5](#) lists the provisioning functions that are available with this connector.

Table 1-5 Provisioning Functions

| Function  | Adapter          | Description   |
|---|------------------|---|
| Create User   | LNCreateUser     | Use this function to create users. Parameters include: <ul style="list-style-type: none"> <li>• <b>objectType</b>: Defined as a constant String, set to the User value.</li> <li>• <b>itResourceFieldValue</b>: Defined as a String, set to UD_LOTUS_SERVERNAME.</li> <li>• <b>processInstanceKey</b>: Defined as a Long, set to Process Instance.</li> </ul>   |
| Delete User   | LNDeleteUser     | Use this function to delete users. Parameters include: <ul style="list-style-type: none"> <li>• <b>objectType</b>: Defined as a String, set to User.</li> <li>• <b>itResourceFieldValue</b>: Defined as a String, set to UD_LOTUS_SERVERNAME.</li> <li>• <b>processInstanceKey</b>: Defined as a Long, set to Process Instance.</li> </ul>  |
| * Updated Where * is the form field label (except Password) | LNUpdateUserInfo | Use this function to update the User field. Parameters include: <ul style="list-style-type: none"> <li>• <b>objectType</b>: Defined as a String, set to User.</li> <li>• <b>itResourceFieldValue</b>: Defined as a String, set to UD_LOTUS_SERVERNAME.</li> <li>• <b>processInstanceKey</b>: Defined as a Long, set to Process Instance.</li> <li>• <b>attrName</b>: Defined as the label of the form field to be updated.</li> </ul>   |
| Password Updated  | LNUpdatePassword | Use this function to update passwords. Parameters include: <ul style="list-style-type: none"> <li>• <b>objectType</b>: Defined as a String, set to User.</li> <li>• <b>itResourceFieldValue</b>: Defined as a String, set to UD_LOTUS_SERVERNAME.</li> <li>• <b>processInstanceKey</b>: Defined as a Long, set to Process Instance.</li> <li>• <b>attrName</b>: Defined as the field to update Password.</li> <li>• <b>oldPassword</b>: Defined as the old password value.</li> </ul> |
| Disable User  | LNDisableUser    | Use this function to set a user's status to disabled. Parameters include: <ul style="list-style-type: none"> <li>• <b>itResourceFieldValue</b>: Defined as a String, set to UD_LOTUS_SERVERNAME.</li> <li>• <b>processInstanceKey</b>: Defined as a Long, set to Process Instance.</li> </ul>   |
| Enable User   | LNEnableUser     | Use this function to set a user's status to enabled. Parameters include: <ul style="list-style-type: none"> <li>• <b>itResourceFieldValue</b>: Defined as a String, set to UD_LOTUS_SERVERNAME.</li> <li>• <b>processInstanceKey</b>: Defined as a Long, set to Process Instance.</li> </ul>  |

### 1.7.3 Reconciliation Rule for Target Resource Reconciliation

Learn about the reconciliation rule for this connector and how to view it.

- [Target Resource Reconciliation Rule](#)

- [Viewing Target Resource Reconciliation Rules](#)

### 1.7.3.1 Target Resource Reconciliation Rule

The following is the process matching rule:

**Rule name:** Reconcile Lotus User

**Rule element:** (Last Name Equals Last Name) AND (First Name Equals First Name)

In the first rule component:

- Last Name to the left of the Equals is the LastName field on the OIM User form.
- LastName to the right of the Equals is the LastName field of the target system.

In the second rule component:

- First Name to the left of the Equals is the FirstName field on the OIM User form.
- First Name to the right of the Equals is the FirstName field of the target system.

### 1.7.3.2 Viewing Target Resource Reconciliation Rules

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

 **Note:**

Perform the following procedure only after the connector is deployed.

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

**Figure 1-2 Reconciliation Rule for Target Resource Reconciliation**

**Reconciliation Rule Builder**

Name:  Operator:  Valid  Active

Object:   AND  OR

For User  For Organization

Description:

---

**Rule Elements**

**Rule Definition**

Buttons: Add Rule, Add Rule Element, Delete, Legend

Tree Structure:

- Rule: Reconcile Lotus User
  - Last Name Equals Last Name
  - First Name Equals First Name

## 1.7.4 Reconciliation Action Rules for Target Resource Reconciliation

Learn about the reconciliation action rules for this connector and how to view them.

- [Target Resource Reconciliation Action Rules](#)
- [Viewing Target Resource Reconciliation Action Rules](#)

### 1.7.4.1 Target Resource Reconciliation Action Rules

[Table 1-6](#) lists the action rules for target resource reconciliation.

**Table 1-6 Action Rules for Target Resource Reconciliation**

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

**Note:**

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

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

### 1.7.4.2 Viewing Target Resource Reconciliation Action Rules

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

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

**Figure 1-3 Reconciliation Action Rules for Target Resource Reconciliation**

| Resource Object                       |   | Object Reconciliation  |                      |      |
|---------------------------------------|---|--|----------------------|------|
|                                       |   | Object Initial Reconciliation Date                           | <input type="text"/> |      |
|                                       |   | <input type="button" value="Create Reconciliation Profile"/> |                      |      |
| Reconciliation Fields                 |   | Reconciliation Action Rules                                  |                      |      |
| <input type="button" value="Add"/>    |   | Rule Condition   | Action               | User |
| <input type="button" value="Delete"/> | 1 | One Process Match Found                                      | Establish Link       |      |
|                                       | 2 | One Entity Match Found                                       | Establish Link       |      |
|                                       | 3 | No Matches Found   | Create User          |      |

## 1.8 Connector Objects Used in the Trusted Source Mode

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

This section discusses the following topics:

- [User Attributes for Trusted Source Reconciliation](#)
- [Reconciliation Rule for Trusted Source Reconciliation](#)
- [Reconciliation Action Rules for Trusted Source Reconciliation](#)

## 1.8.1 User Attributes for Trusted Source Reconciliation

The Lookup.Domino.UM.ReconAttrMap.Trusted lookup definition (see [Table 1-2](#)) maps resource object fields and target system attributes. The Code Key column stores the names of resource object fields. The Decode column:

[Table 1-7](#) provides information about the form fields used for trusted source reconciliation.

**Table 1-7 OIM User Fields Used for Trusted Source Reconciliation**

| Process Form Field | Field Type | Description  |
|--------------------|------------|--|
| Email              | TextField  | E-mail address   |
| First Name         | TextField  | First name   |
| Last Name          | TextField  | Last name  |
| Middle Name        | TextField  | Middle name  |
| Status             | TextField  | Reconciliation status                                  |
| User Login         | TextField  | 16-bit alphanumeric ID that uniquely identifies a user |

[Table 1-8](#) lists the form field and user attribute mappings for trusted source reconciliation.

**Table 1-8 Mapping Form Fields to User Attributes for Trusted Source Reconciliation**

| OIM User Form Field | IBM Lotus Notes and Domino Attribute |
|---------------------|--------------------------------------|
| Status[TRUSTED]     | _ENABLE_                             |
| User Login          | ShortName                            |
| First Name          | FirstName                            |
| Email               | InternetAddress                      |
| Middle Name         | MiddleInitial                        |
| Last Name           | LastName                             |

## 1.8.2 Reconciliation Rule for Trusted Source Reconciliation

Learn about the reconciliation rule for trusted source reconciliation and how to view it.

- [Trusted Source Reconciliation Rule](#)
- [Viewing Trusted Source Reconciliation Rule](#)

### 1.8.2.1 Trusted Source Reconciliation Rule

The following is the process matching rule:



**Rule name:** Lotus Trusted User

**Rule element:** User Login equals User Login

### 1.8.2.2 Viewing Trusted Source Reconciliation Rule

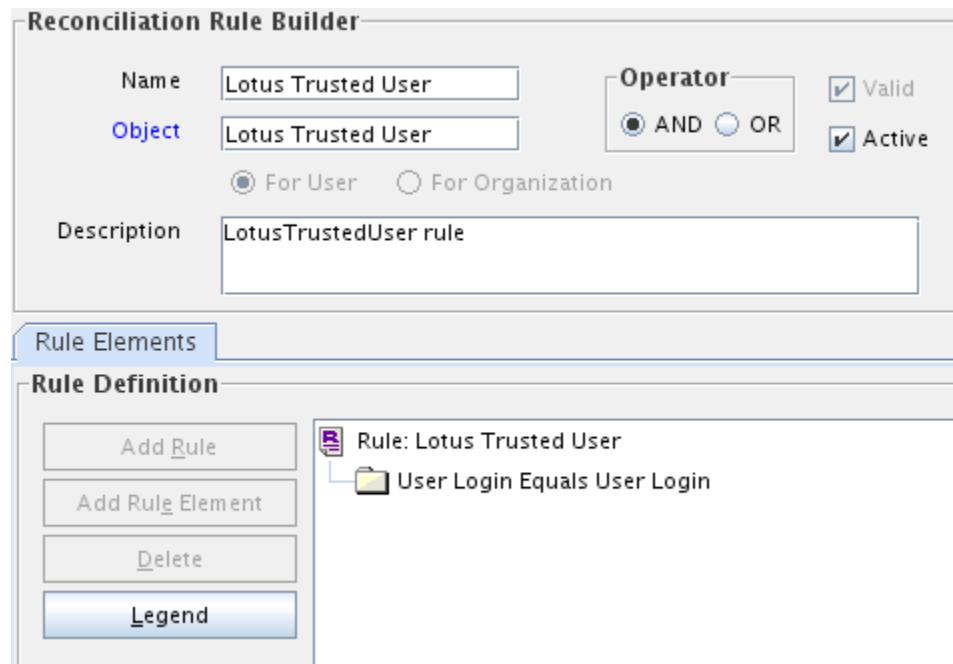
After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

 **Note:**

Perform the following procedure only after the connector is deployed.

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **Lotus Trusted User**.

**Figure 1-4 Reconciliation Rule for Trusted Source Reconciliation**



### 1.8.3 Reconciliation Action Rules for Trusted Source Reconciliation

Learn about the reconciliation action rules for trusted source reconciliation and how to view them.

- [Trusted Source Reconciliation Action Rules](#)
- [Viewing Trusted Source Reconciliation Action Rules](#)

### 1.8.3.1 Trusted Source Reconciliation Action Rules

Table 1-9 lists the action rules for trusted source reconciliation.

**Table 1-9 Action Rules for Trusted Source Reconciliation**

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

 **Note:**

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

- [Setting a Reconciliation Action Rule \(Developing Identity Connectors Using Java\)](#)
- [Setting a Reconciliation Action Rule \(Developing Identity Connectors Using .NET\)](#)

### 1.8.3.2 Viewing Trusted Source Reconciliation Action Rules

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

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

**Figure 1-5 Reconciliation Action Rules for Trusted Source Reconciliation**

The screenshot shows a software interface for configuring reconciliation rules. At the top, there are two tabs: 'Resource Object' and 'Object Reconciliation'. Below the 'Object Reconciliation' tab, there is a field for 'Object Initial Reconciliation Date' and a button labeled 'Create Reconciliation Profile'. Below this, there are two sub-tabs: 'Reconciliation Fields' and 'Reconciliation Action Rules'. The 'Reconciliation Action Rules' sub-tab is active, displaying a table with three columns: 'Rule Condition', 'Action', and 'User'. To the left of the table are two buttons: 'Add' and 'Delete'. The table contains three rows of data:

|   | Rule Condition          | Action         | User |
|---|-------------------------|----------------|------|
| 1 | One Process Match Found | Establish Link |      |
| 2 | One Entity Match Found  | Establish Link |      |
| 3 | No Matches Found        | Create User    |      |

# 2

## Deploying the Connector

The procedure to deploy the connector is divided across three stages namely preinstallation, installation, and postinstallation.

- [Preinstallation](#)
- [Installation](#)
- [Postinstallation](#)

This chapter also includes information about:

- [Upgrading the Connector](#)
- [Defining a Connector](#)

### 2.1 Preinstallation

Preinstallation involves copying external code files to a given location on the computer hosting the connector server, and then creating a target system account for performing connector operations.

This section is divided into the following topics:

- [Understanding the Connector Deployment Architecture](#)
- [Files and Directories on the Connector Installation Media](#)
- [Using External Code Files](#)
- [Creating a Target System Account for Connector Operations](#)

 **Note:**

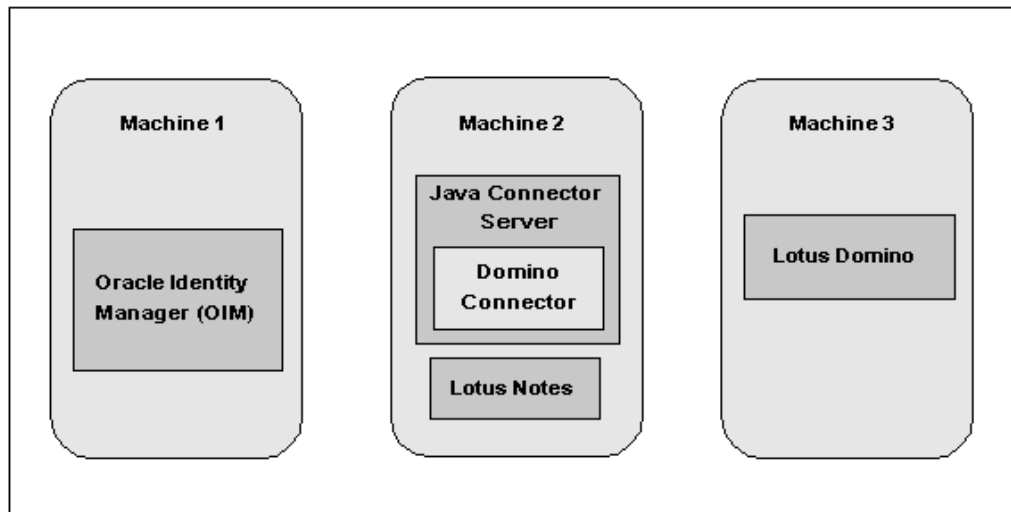
You must install single user notes client only on the connector server machine.

#### 2.1.1 Understanding the Connector Deployment Architecture

The Lotus Notes/Domino connector requires a distributed deployment architecture.

[Figure 2-1](#) shows the architecture required for deploying the connector.

Figure 2-1 Connector Deployment Architecture



- **Machine 1** has Oracle Identity Manager deployed.

 **Note:**

Deploying the Lotus Notes/Domino connector on the Oracle Identity Manager computer is not certified. You must deploy the Domino Identity Connector bundle in the Java Connector Server (Machine 2 in the figure).

- **Machine 2** has the Lotus Notes/Domino connector and the Java Connector Server deployed.

You must install the Java Connector Server and the Lotus Notes client on the same computer where you deploy the Lotus Notes/Domino connector.

Since the connector binary is dependent on Lotus Notes client and the latter is only available in 32-bit version, we can not release 64-bit binary for the connector. The Domino connector uses the 32-bit Domino C API and therefore is supported only with the 32-bit version of Lotus Notes, so you must deploy 32-bit notes client. Both windows and Linux Os are supported.

 **Note:**

See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing and configuring a connector server and about running the connector server.

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

- **Machine 3** has the Domino target deployed.

## 2.1.2 Files and Directories on the Connector Installation Media

These are the list of files and directories in the connector installation media and their descriptions.

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

**Table 2-1 Files and Directories On the Connector Installation Media**

| File in the Installation Media Directory             | Description  |
|--|--|
| <code>org.identityconnectors.domino-2.0.2.jar</code> | This JAR file contains the Domino Identity Connector bundle that must be deployed into the connector server before you can install the OIM Lotus Notes/Domino connector.   |
| <code>configuration/IBMLotusDomino-CI.xml</code>     | This XML file contains configuration information that is used during connector installation.   |
| <code>xml/Domino-Datasets.xml</code>                 | This file, used in conjunction with the OIM Import Deployment Manager file, contains the parameters necessary to import the datasets for request-based provisioning.   |
| <code>resources/</code>                              | This directory contains all of the resource bundles with language-specific information that is used by the connector. During connector deployment, these resource bundles are copied to the Oracle Identity Manager database.<br><b>Note:</b> A <b>resource bundle</b> is a file containing localized versions of the text strings that include GUI element labels and messages. |
| <code>test-utility/example-config.groovy</code>      | This file contains an example that you can modify to test basic provisioning operations.   |
| <code>test-utility/test-utility.jar</code>           | This jar file contains a utility used to test basic provisioning operations (create, update, and delete) on a configurable target resource.  |
| <code>xml/Domino-ConnectorConfig.xml</code>          | This XML file contains definitions for the following components of the connector: <ul style="list-style-type: none"> <li>• IT resource type</li> <li>• IT resource</li> <li>• Resource object</li> <li>• Process definition</li> <li>• Process tasks</li> <li>• Adapters</li> <li>• Process form</li> <li>• Lookup definitions</li> </ul>  |

## 2.1.3 Using External Code Files

Ensure you have the `Notes.jar` file available. This file comes packaged with the IBM Lotus Notes software.

Copy the `Notes.jar` file from the `LOTUS_HOME/Domino/jvm/lib/ext` directory into the `CONNECTOR_SERVER_HOME/lib` directory.

Here, `LOTUS_HOME` is the directory in which IBM Lotus Notes and Domino is installed and `CONNECTOR_SERVER_HOME` is the directory in which the connector server is installed.

[Testing the Connector](#) describes the procedure to use the testing utility. Before running the testing utility, copy the `Notes.jar` files into the `OIM_HOME/server/ThirdParty` directory.

## 2.1.4 Creating a Target System Account for Connector Operations

Oracle Identity Manager uses a target system user account to provision to, and reconcile data from, the target system. See the target system documentation for creating a target system account.



### Note:

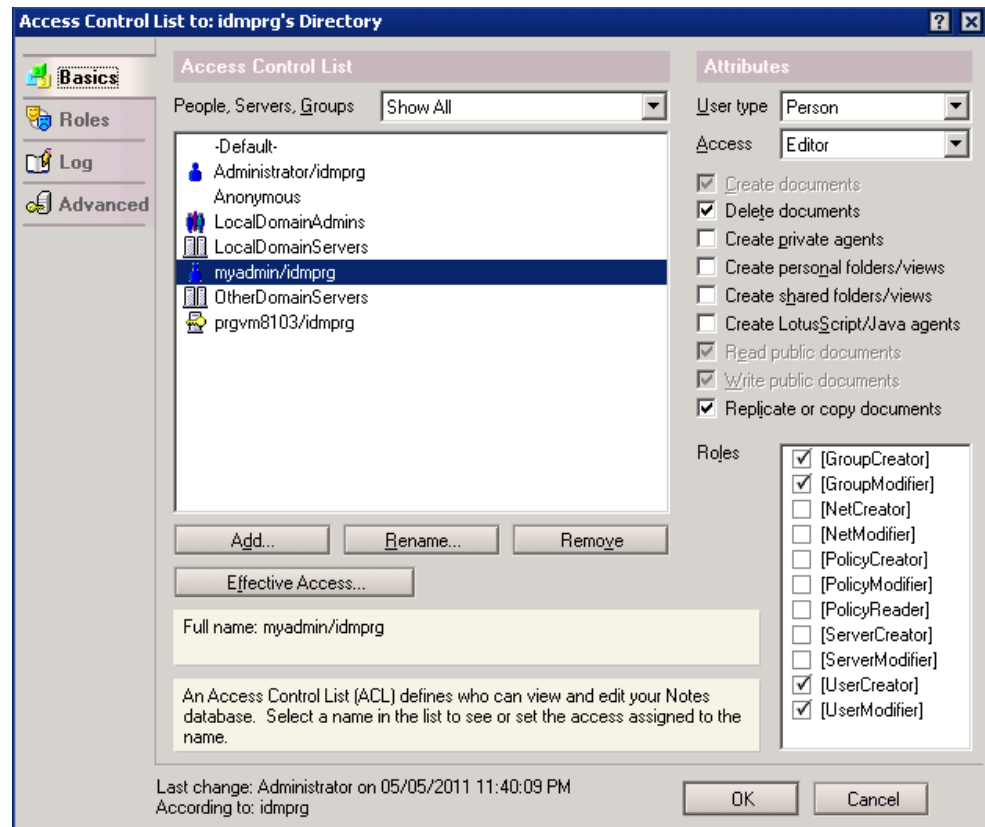
To perform the procedure described in [Configuring the IT Resource](#), the user must be "Administrator." In addition, if Lotus scripts are used in pre-actions or post-actions, the user must also have "Sign or run restricted LotusScript/Java agents" rights.

For IBM Lotus Notes and Domino, the user must have the minimum rights for provisioning/reconciliation. Use the following procedure to specify the minimum rights required for the Domino administrator:

1. Create the Identity Manager administrator in Domino. Use a certifier ID that has access to all organizations needed to manage users.
2. Add the user to the access control list (ACL) of the address book for the server, `names.nsf`.
  - a. Give the user Editor access.
  - b. Assign the user the following roles:
    - GroupModifier
    - UserCreator
    - UserModifier
  - c. Ensure the user has the following rights:
    - Create documents, Delete documents, Read public documents, Write public documents, and Replicate or Copy documents

These selections are illustrated in [Figure 2-2](#).

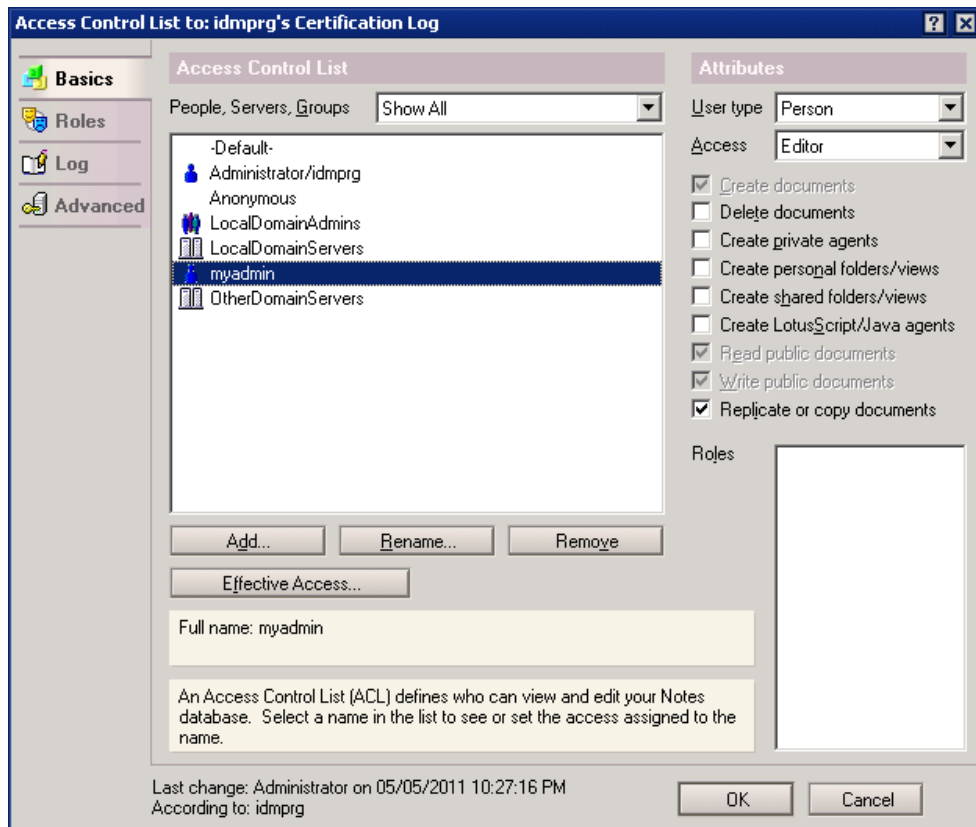
Figure 2-2 Adding User to the ACL



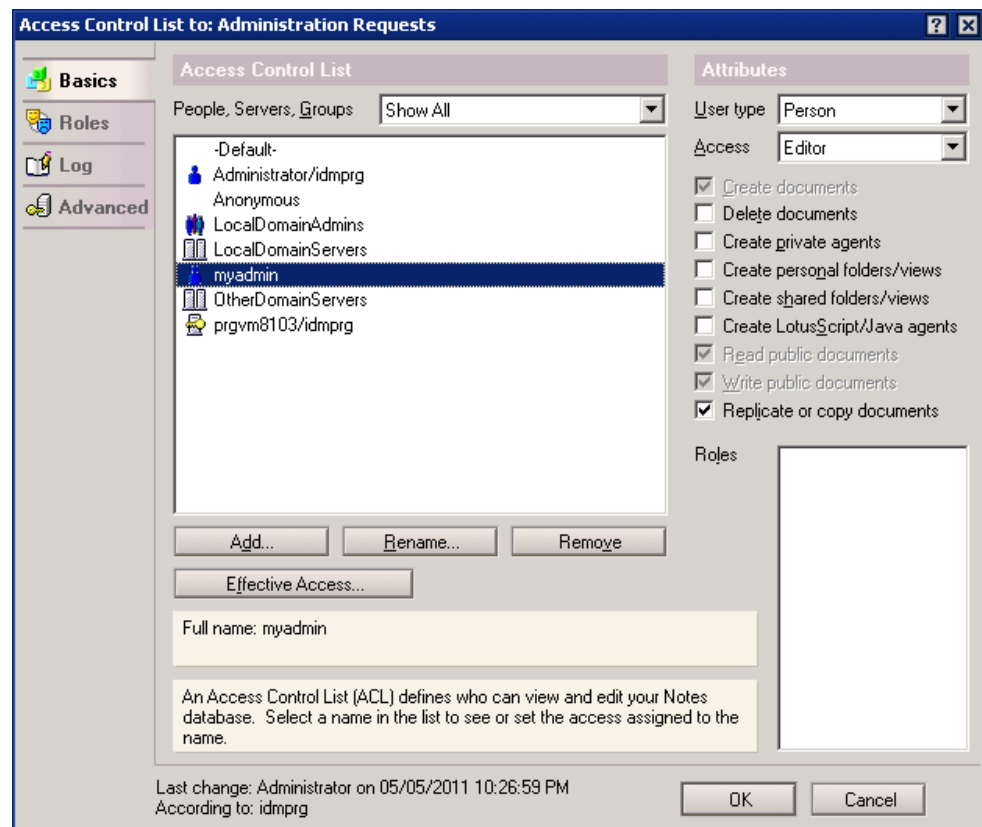
3. Add the user to the registration log ACL, `certlog.nsf`, with Editor access. For example, see [Figure 2-3](#).



Figure 2-3 Adding User to the Registration Log ACL



4. Add the user to the Administration Requests ACL, `admin4.nsf`, with Editor access as illustrated in [Figure 2-4](#).

**Figure 2-4 Adding User to the Administration Requests ACL**

5. Add the newly created user to the server security by opening the Security panel and editing the server configuration as follows:
  - If access to the Domino server is restricted, ensure the Identity Manager account has access to the server by specifying the account name (or a group to which the account belongs) in the Access Server field.
  - If a before or after action calls a Domino agent, you might have to add the user to the Run unrestricted LotusScript/Java agents or Run restricted LotusScript/Java agent field, depending on how the agent being called is configured.

## 2.2 Installation

Installing the connector involves the following procedures:

- [Installing the Domino Identity Connector on the Connector Server](#)
- [Running the Connector Installer](#)
- [Configuring the IT Resource](#)

### 2.2.1 Installing the Domino Identity Connector on the Connector Server

Before installing the OIM Lotus Notes/Domino connector, you must install the Domino Identity Connector (bundle/org.identityconnectors.domino-2.0.1.jar in the installation media directory) into the Java Connector Server.

 **Note:**

- You can download the Java Connector Server from the Oracle Technology Network web page.
- For information about installing, configuring, and running a connector server, see *Using an Identity Connector Server in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

To do so:

1. Stop the Java Connector Server.
2. Copy the Domino connector bundle into the Java Connector Server `CONNECTOR_SERVER_HOME\bundles` directory.
3. Copy the `Notes.jar` file from the Lotus Notes installation directory to the `CONNECTOR_SERVER_HOME\lib` directory.
4. Ensure that the `PATH` variable specifies the directory where `nnotes.dll` resides.

 **Note:**

You must switch Lotus Notes to the user ID configured in OIM for provisioning *before* starting the Connector Server or error messages will result.

5. Start the Java Connector Server.

## 2.2.2 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:  
`OIM_HOME/server/ConnectorDefaultDirectory`

 **Note:**

In an Oracle Identity Manager cluster, you must copy these files to each node in the cluster.

2. If you are using Oracle Identity Manager release 11.1.1.x, then:
  - a. Log in to Oracle Identity Manager Administrative and User Console by using the user account described in *Creating the User Account for Installing Connectors of Oracle Fusion Middleware Administering Oracle Identity Manager*.
  - b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.

3. If you are using Oracle Identity Manager release 11.1.2.x, then:
  - a. Log in to Oracle Identity System Administration by using the user account described in *Creating the User Account for Installing Connectors of Oracle Fusion Middleware Administering Oracle Identity Manager*.
  - b. In the left pane, under System Management, click **Manage Connector**.
4. In the Manage Connector page, click **Install**.
5. 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 in Step 1.

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

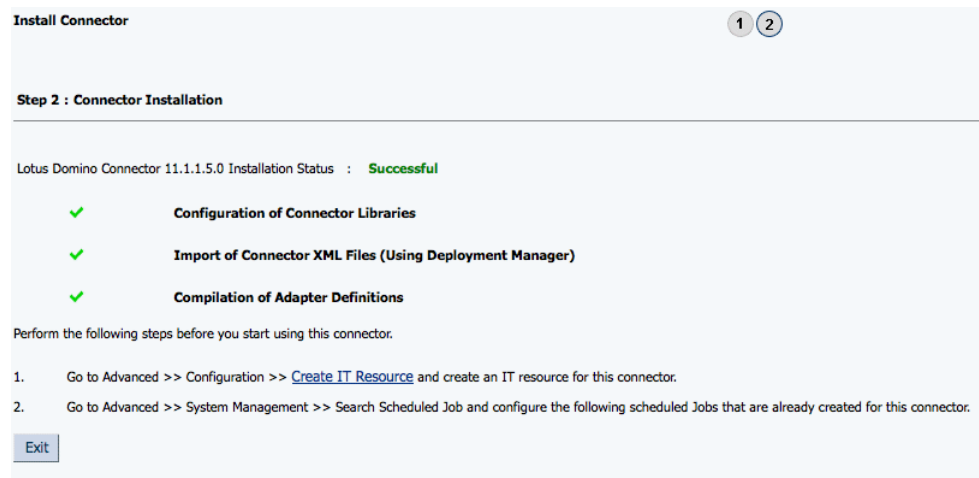
- a. In the **Alternative Directory** field, enter the full path and name of that directory.
  - b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
  - c. From the Connector List list, select **IBM Lotus Notes Domino RELEASE\_NUMBER**.
6. Click **Load**.
7. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager).
- c. Compilation of adapters

On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

- Retry the installation by clicking **Retry**.
  - Cancel the installation and begin again from Step 1.
8. 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.

**Figure 2-5 Connector Installation Success Screen**

These steps are as follows:

- Ensuring that the prerequisites for using the connector are addressed

 **Note:**

At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See [Clearing Connector Resource Bundles Content from the Server Cache](#) for information about running the PurgeCache utility.

There are no prerequisites for some predefined connectors.

- 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.

- Configuring the scheduled jobs that are created when you installed the connector

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

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

If you are installing Oracle Identity Manager in a cluster, then you must copy all the JAR files and the contents of the `connectorResources` directory into the corresponding directories on each node of the cluster. See [Table 2-1](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

## 2.2.3 Configuring the IT Resource

The IT resource for the target system is created during connector installation. This IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

You can use one of the following methods to configure an IT resource:

- [Edit an Existing IT Resource Instance](#)
- [Create a New IT Resource](#)

### Note:

If you have configured your target system as a trusted source, then create an IT resource of type **Lotus Notes**. For example, Lotus Notes Trusted. The parameters of this IT resource are the same as the parameters of the IT resources described in [Table 2-2](#) of this section.

For either method, specify the parameters for the resource, as described in [Parameters of the IT Resource](#), as appropriate for your environment.

### 2.2.3.1 Parameters of the IT Resource

[Table 2-2](#) describes the parameters of the IT resource for the target system.

**Table 2-2 IT Resource Parameters**

| Parameter            | Description   |
|----------------------|---|
| useCAProcess         | Set the value of this parameter to <code>true</code> if you are using CA Certificates. Otherwise, set the value of this parameter to <code>false</code> .<br>Default is: <code>false</code> . |
| caCertifierName      | Enter the hierarchical CA Certifier name here.<br>For example: <code>/ca/org1</code><br>In this example, CA is the CA Certifier under org1 organization.                                      |
| adminIdFile          | Fully-qualified path to the Administrator ID file.<br>For example: <code>C:\Lotus\Notes\Data\admin.id</code>  |
| adminName            | Administrator account name, such as Administrator/ACM   |
| adminPassword        | Administrator password.   |
| administrationServer | For Notes User: Name of the host where the administration server is running.<br>For Web User: Canonical name of the administration server. For example : <code>CN=Myserver/O=org</code>       |
| certifierIdFile      | Fully-qualified path to the Certifier ID file.<br>For example: <code>C:\Lotus\Domino\Data\cert.id</code>  |
| certifierPassword    | Password for the specified Certifier ID file.   |

Table 2-2 (Cont.) IT Resource Parameters

| Parameter            | Description   |
|----------------------|---|
| Configuration Lookup | Name of the Lookup definition containing the configuration information.<br>Values can be: <ul style="list-style-type: none"> <li>Lookup.Configuration.Domino for Target Reconciliation</li> <li>Lookup.Configuration.Domino.Trusted for Trusted Reconciliation</li> </ul> <b>Note:</b> If you create another lookup definition in which to store connector configuration parameters, then specify the name of the new lookup definition as the value of this parameter. |
| ConnectorServerName  | Enter the name of the host where the connector server is running.<br>Name of the IT resource for the Connector Server. You create an IT resource for the Connector Server in <a href="#">Creating the IT Resource for the Connector Server</a> .<br><b>Note:</b> Enter a value for this parameter <i>only</i> if you have deployed the Lotus Notes/Domino connector in the Connector Server.  |
| deleteDenyGroup      | Enter the name of the Deleted User group to which users who are deleted must be assigned.   |
| disableDenyGroup     | Specify to disable user accounts in the connector. Not returned by default.<br>When you disable a user account, the user automatically becomes a member of a Deny Access group. Re-enable the user account to remove the user from the Deny Access group.<br><b>Note:</b> To create a Deny List group on the Domino installation, you must create the group in the IT resource. Refer to " <a href="#">Configuring the Target System</a> " for instructions.            |
| idType               | Type of ID file: <ul style="list-style-type: none"> <li>Specify 0 for flat</li> <li>Specify 1 for hierarchical</li> </ul> Default is: 0   |
| MailReplicaServer    | Specifies the names of servers to which the mail database will replicate.<br>Use this value only when registering new users. You cannot update this value and it is not reconciled.   |
| mailServer           | Default mail server to use when creating users. Use the abbreviated format. For example: <code>server/org</code><br>Only one mail server is supported at a time, but you can change servers if necessary.   |
| mailSystem           | Indicates the default mail system when creating users:<br>Specify one of the following values: <ul style="list-style-type: none"> <li>0: Notes</li> <li>1: CCMAIL</li> <li>2: VIMMail</li> <li>99: None</li> </ul> Default is: 0  |
| mailTemplateName     | Name of mail template. Valid only during create.  |
| policy               | Specify the name of the Domino explicit policy to be assigned to the user. When set, this value could modify or override other user attribute values. Refer to the Domino documentation for more information.   |
| registrationLog      | Enter the name of the log file to be used when creating IDs.<br>Default is: <code>C:/Lotus/Domino/Data/certlog.nsf</code>   |

**Table 2-2 (Cont.) IT Resource Parameters**

| Parameter          | Description   |
|--------------------|---|
| registrationServer | Enter the canonical name of the server to be used when creating IDs and performing other registration functions.<br>Sample value: CN=MyServer/OU=MyOrg  |
| roamCleanPer       | If the value of Roaming Cleanup is 1, specifies the period in days that cleanup will be performed.  |
| roamCleanSetting   | Cleanup setting for files belonging to roaming Domino accounts. Values can be: <ul style="list-style-type: none"> <li>• <b>0</b>: Never</li> <li>• <b>1</b>: Periodically in days</li> <li>• <b>2</b>: At shutdown</li> <li>• <b>3</b>: Prompt</li> </ul> |
| roamRplSrvrs       | List of servers that will contain replicas of roaming files.  |
| roamSrvr           | Server destination for roaming files belonging to a Domino account.   |
| userDatabaseName   | Specify the filename of the user database.<br><b>Note:</b> This parameter does not support secondary directory. Instead, only read/write data from/into the primary directory ( =names.nsf ) is supported.  |

### 2.2.3.2 Edit an Existing IT Resource Instance

To simplify the IT resource configuration process, the IBM Lotus Notes and Domino connector provides two empty IT Resource instances:

- **Lotus Domino** for configuring the target system as a managed (target) resource
- **Lotus Domino Trusted** for configuring the target system as an authoritative (trusted) source

#### Note:

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

You can use either instance to configure an IT resource by editing the parameter values to suit your deployment requirements.

1. If you are using Oracle Identity Manager release 11.1.1.x, then:
  - a. Log in to the Administrative and User Console.
  - b. On the Welcome page, open **Manage IT Resource** in the upper-right corner of the page.
2. If you are using Oracle Identity Manager release 11.1.2.x or later, then:
  - a. Log in to Identity System Administration.
  - b. In the left pane, under Provisioning Configuration, click **IT Resource**.
3. In the **IT Resource Type** combo box, select **Lotus Notes**, and then click **Search**.



The **Lotus Domino** and **Lotus Domino Trusted** IT resource types are displayed.

4. Select one of these resource types and then click **Edit** to modify the necessary IT Resource parameters.

For a description of the different IT resource parameters, refer to [Table 2-2](#).

### 2.2.3.3 Create a New IT Resource

To create a new Lotus Notes IT resource and specify values for the parameters for that resource, follow these steps:

1. If you are using Oracle Identity Manager release 11.1.1.x, then:
  - a. Log in to the Administrative and User Console.
  - b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.
2. If you are using Oracle Identity Manager release 11.1.2.x or later, then:
  - a. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see *Managing Sandboxes of Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
  - b. In the left pane, under Configuration, click **IT Resource**.
3. Provide an IT Resource value.
4. Click the Search icon and select **Lotus Notes**, or type **Lotus Notes** directly into the IT Resource Type field.

The **Lotus Domino** and **Lotus Domino Trusted** IT resource types are displayed.

5. Select one of the IT resource type options and then click **Continue**.
6. Specify values for the parameters of the IT resource.

For a description of the different IT resource parameters, refer to [Table 2-2](#).

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

## 2.3 Postinstallation

Postinstallation involves performing certain procedures such as configuring Oracle Identity Manager, creating the IT resource for the Connector Server, enabling the Reset Password option, localizing field labels, and so on.

The following sections discuss postinstallation procedures:

- [Configuring Oracle Identity Manager 11.1.2 or Later](#)
- [Localizing Application Instance Form](#)
- [Enabling the Reset Password Option in Oracle Identity Manager 11.1.2 or Later](#)
- [Configuring Oracle Identity Manager](#)
- [Configuring the Target System](#)
- [Creating the IT Resource for the Connector Server](#)

## 2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

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

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Creating an Application Instance](#)
- [Publishing a Sandbox](#)
- [Harvesting Entitlements and Sync Catalog](#)
- [Updating an Existing Application Instance with a New Form](#)

### 2.3.1.1 Creating and Activating a Sandbox

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

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

### 2.3.1.2 Creating a New UI Form

Create a new UI form as follows.

1. In the left pane, under Configuration, click **Form Designer**.
2. Under Search Results, click **Create**.
3. Select the resource type for which you want to create the form, for example, Lotus Notes User.

4. Enter a form name and click **Create**.

### 2.3.1.3 Creating an Application Instance

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

1. In the System Administration page, under Configuration in the left pane, click **Application Instances**.
2. Under Search Results, click **Create**.
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save**.
4. In the Form drop-down list, select the newly created form and click **Apply**.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See *Managing Organizations Associated With Application Instances in Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed instructions.

### 2.3.1.4 Publishing a Sandbox

To publish the sandbox that you created in [Creating and Activating a Sandbox](#):

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

### 2.3.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

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

### 2.3.1.6 Updating an Existing Application Instance with a New Form

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

1. Create a sandbox and activate it as described in [Creating and Activating a Sandbox](#).
2. Create a new UI form for the resource as described in [Creating a New UI Form](#).
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created. You must first refresh to populate the new form in the list.
5. Save the application instance.
6. Publish the sandbox as described in [Publishing a Sandbox](#).

## 2.3.2 Localizing Application Instance Form

To localize the application instance form:

1. Publish the sandbox containing application instance form that is supposed to be localized.
2. Export the MDS file, `"/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"`.

In this file, you can see message keys and messages to be localized.

```
sessiondef.oracle.iam.ui.runtime.form.model.testAppInstance.entity.testAppInstanceEO.UD_TES8393_ACCOUNTID__c_LABEL
```

### See Also:

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

3. Export the file to localize, for example, for German:

```
/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle_de.xlf
```

### Note:

This file may not exist in MDS. If it does not exist, create a new one, but path must be the same.

4. Provide localization for messages in German, follow the same format as in the file exported in step 2.

### See Also:

Translating Resource Bundles from an MDS Repository in *Oracle Fusion Applications Extensibility Guide* for more information about translating resource bundles from metadata services metadata repository

5. Import `/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle_de.xlf` back to MDS.
6. Logout and relogin.

## 2.3.3 Enabling the Reset Password Option in Oracle Identity Manager 11.1.2 or Later

In Oracle Identity Manager 11.1.2 or later, you can reset password for an account after logging in as the user by navigating to My Access, Accounts tab. The Reset Password option is enabled for only those accounts that follow the `UD_FORMNAME_PASSWORD` naming convention for the password field.

### Note:

In Oracle Identity Manager 11.1.2 prior to release 11.1.2.1.0, if you want to change the password of a Lotus Notes account under My Information, the account is not available for selection in the drop-down list of accounts. See bug 16483800 in [Known Issues and Workarounds](#) for more information about this known issue.

To enable the Reset Password option in Oracle Identity Manager 11.1.2.x or later:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click **Form Designer**.
3. Enter `UD_LOTUS` in the Table Name field and click the **Query for records** button.
4. Click **Create New Version**.
5. In the Create a New Version dialog box, specify the version name in the Label field, save the changes, and then close the dialog box.
6. From the **Current Version** list, select the newly created version.
7. Delete the existing label `UD_LOTUS_USERPWS` and add a similar label as `UD_LOTUS_PASSWORD` with similar values for all columns.
8. Save and Click on **Make Version Active**.
9. Close the Form Designer.
10. In the left pane, under Process Management, Click **Process Definition**.
11. Enter Lotus User in Name field and Click the **Query for records** button.
12. Open the Password Updated task.
13. Click **integration tab**.
14. Perform the following steps:
  - a. Click and open **fieldName** and change Literal Value to `UD_LOTUS_PASSWORD`.
  - b. Save and close.

 **Note:**

If password Updated task fails after these steps, you might be encountering cache issue. As a work around, you must do these steps:

- i. Click and open **fieldValue** and toggle Qualifier value to something other than Password (for example: ID File Name) and save it. Again Revert it back to Password. Save and close.
- ii. Click and open **fieldOldValue** and toggle Qualifier value to something other than Password (for example: ID File Name) and save it. Again Revert it back to Password. Save and close.

15. Update the application instance with the new form as described in [Updating an Existing Application Instance with a New Form](#) .
16. Run *FVC utility* from *OIM\_HOME/designconsole* with proper from and to version of the Form.
17. Access OIM DB and run following sql script to make necessary changes to already existing users:  

```
update UD_LOTUS set UD_LOTUS_PASSWORD=UD_LOTUS_USERPWS;
```

## 2.3.4 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

 **Note:**

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

- [Setting Up the Lookup.Configuration.Domino Lookup Definition](#)
- [Configuring Trusted Source Reconciliation](#)
- [Changing to the Required Input Locale](#)
- [Clearing Connector Resource Bundles Content from the Server Cache](#)
- [Enabling Logging in the Java Connector Server](#)
- [Enabling Request-Based Provisioning](#)

### 2.3.4.1 Setting Up the Lookup.Configuration.Domino Lookup Definition

The Lookup.Configuration.Domino lookup definition is created when you deploy the connector. You must set values for some of the entries in this lookup definition. To set values for these entries:

1. On the Design Console, expand **Administration** and then double-click **Lookup Definition**.
2. Search for and open the **Lookup.Configuration.Domino** lookup definition.

3. Set values for the entries specified in [Table 2-3](#).

 **Note:**

You must not change any of the Code Key values of this lookup definition.

**Table 2-3 Entries in the Lookup.Configuration.Domino Lookup Definition**

| Code Key       | Decode Description   |
|----------------|--|
| Bundle Name    | This entry holds the name of the connector bundle class. <i>Do not modify this entry.</i>    |
| Bundle Version | This entry holds the version of the connector bundle class. <i>Do not modify this entry.</i> |
| Connector Name | This entry holds the name of the connector class. <i>Do not modify this entry.</i>           |

### 2.3.4.2 Configuring Trusted Source Reconciliation

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

 **Note:**

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

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

1. Create a new Lotus Notes-type IT resource as described in [Configuring the IT Resource](#).
2. Configure the new IT resource properly by using resource parameters that are appropriate for your environment. This configuration is similar to configuring a non-trusted resource.)
3. Set the Configuration Lookup parameter value to **Lookup.Configuration.Domino.Trusted**.
4. Search for the Domino Connector Trusted User Reconciliation scheduled task and set the IT Resource Name value to the name of the IT Resource you just configured in the preceding steps.

Trusted reconciliation should now be configured properly.

### 2.3.4.3 Changing to the Required Input Locale

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

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

### 2.3.4.4 Clearing Connector Resource Bundles Content from the Server Cache

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the Oracle Identity Manager database. Whenever you add a new resource bundle to the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, switch to the `OIM_HOME/server/bin` directory.

 **Note:**

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

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

2. Enter the following command:

 **Note:**

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

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

```
PurgeCache.bat MetaData
```

On Microsoft Windows: `PurgeCache.bat All`

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

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

In this format:

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



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

### 2.3.4.5 Enabling Logging in the Java Connector Server

The Connector Server logging is controlled by the `logging.properties` file under the `CONNECTOR_SERVER_HOME/conf` folder. This file can be used to edit the properties to enable logging. To do so, perform the following steps:

1. Open the `logging.properties` file.
2. To enable logging for the Lotus Notes/Domino connector, add `ORG.IDENTITYCONNECTORS.DOMINO.level=FINEST` to the current file.
3. Save and close the file.
4. Restart the Java connector server.
5. The logs will be written to the console or to a file as per the handlers definition.  
By default, the logs can be found in the `logs/connectorserver%u.log` file.

### 2.3.4.6 Enabling Request-Based Provisioning



#### Note:

Perform the procedure described in this section only if you want to enable request-based provisioning.

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



#### Note:

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

Enabling request-based provisioning involves performing the following procedures:

- [Copying Predefined Request Datasets](#)
- [Importing Request Datasets into the MDS](#)
- [Enabling the Auto Save Form Feature](#)
- [Running the PurgeCache Utility](#)

#### 2.3.4.6.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped

with this connector. These datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

Use the Deployment Manager to import the `xml/Domino-Datasets.xml` file supplied with the Lotus Notes/Domino connector zip file. Then, you can use this `xml` file in conjunction with the OIM Import Deployment Manager file, to import the necessary datasets for request-based provisioning.

Depending on your requirements, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets.

### 2.3.4.6.2 Importing Request Datasets into the MDS

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

To import a request dataset definition into the MDS:

1. Set up the environment for running the MDS Import utility as follows:
  - a. Set Environment Variable: Set the `OIM_ORACLE_HOME` environment variable to the Oracle Identity Management Oracle home directory inside the Middleware home directory. For example, for Microsoft Windows, set the `OIM_ORACLE_HOME` environment variable to `C:\Oracle\Middleware\Oracle_IDM1\` directory.
  - b. Set Up the Properties File: Set the necessary properties in the `weblogic.properties` file, which is located in the same folder as the utilities.

#### Note:

While setting up the properties in the `weblogic.properties` file, ensure that the value of the `metadata_from_loc` property is the parent directory of the `/custom/connector/RESOURCE_NAME` directory. For example, while performing the procedure in [Copying Predefined Request Datasets](#), if you copy the files to the `E:\MyDatasets\custom\connector\Exchng` directory, then set the value of the `metada_from_loc` property to `E:\MyDatasets`.

**Table 2-4 Parameters in the Properties File**

| Property Name               | Description   | Notes |
|-----------------------------|---|-------|
| <code>wls_servername</code> | Name of the Oracle WebLogic Server on which Oracle Identity Manager is deployed |       |

**Table 2-4 (Cont.) Parameters in the Properties File**

| Property Name     | Description  | Notes   |
|-------------------|--|---|
| application_name  | The application name   | Value is: <ul style="list-style-type: none"> <li>oim if importing/exporting an out-of-the-box event handler.</li> <li>OIMMetadata for customizable metadata.</li> </ul> If importing or exporting custom data, set application_name to OIMMetadata. |
| metadata_from_loc | Directory location from which an XML file should be imported. This property is used by weblogicImportMetadata.sh script.     | Microsoft Windows paths include // as file or directory separator.  |
| metadata_to_loc   | Directory location from which an XML file should be imported. This property is used by weblogicExportMetadata.sh script.     | Microsoft Windows paths include // as file or directory separator.  |
| metadata_files    | Full path and name of an XML file. This property is used by weblogicExportMetadata.sh and weblogicDeleteMetadata.sh scripts. | For example, you may specify /file/User.xml to export a user entity definition. You can indicate multiple xml files as comma-separated values.  |

2. In a command window, change to the *OIM\_HOME/server/bin* directory.

3. Run the following command:

```
weblogicImportMetadata.bat
```

4. When prompted, enter values for the following:

- Please enter your username [weblogic]

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

Sample value: WL\_User

- Please enter your password [weblogic]

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

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

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

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

In this format, replace:

- *HOST\_NAME\_IP\_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.
- *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into the MDS.

### 2.3.4.6.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

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

### 2.3.4.6.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See [Clearing Connector Resource Bundles Content from the Server Cache](#) for instructions.

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

### 2.3.4.7 Enabling IT Resource Name Values in the Process Form

IT Resource Name values are not populated in the process form after target reconciliation by default. To configure the process form to include these values, perform the following steps:

From the Design Console:

1. Locate the `Lotus User` resource object.
2. Click the **Object Reconciliation** tab.
3. Double-click the **Server name reconciliation** field and change the field name to **IT Resource Name**. Save it.
4. Locate the `Lotus User` process definition.
5. Click the **Reconciliation Field Mapping** tab.
6. Ensure the **IT Resource Name** field is correctly mapped to the `UD_LOTUS_SERVER_NAME`.
7. Return to the `Lotus User` resource object and then to the **Object Reconciliation** tab.
8. Click **Create Reconciliation Profile**.

## 2.3.5 Configuring the Target System

To configure the target system, you must create a Deny Access Group.

This section discusses the following topics:

- [Creating a Deny Access Group](#)
- [Disabling a User Account](#)

### 2.3.5.1 Creating a Deny Access Group

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 **Deny List Only**.
5. Click **Save & Close**.
6. On the Configuration tab, click **All Server Documents** on the left pane.
7. On the right pane, double-click the row for the server that you are using.
8. Open the Security tab.
9. In the Server Access section, double-click **Not Access Server**.
10. In the Select Names dialog box, use the **Add** button to add the group that you create in Step 4 and then click **OK**.
11. Click **Save & Close**.
12. To view the Deny Access group that you created, perform Steps 6 through 9.

### 2.3.5.2 Disabling a User Account

When you configure the IT resource, you specify the name of the Deny Access group (for example, `noaccess`) that you created in Step 4 of [Creating a Deny Access Group](#) as the value of the `disableDenyGroup` IT resource parameter.

To disable a user account in the connector, you specify the `disableDenyGroup` in the IT resource. If this parameter is not set in the IT resource, then when you disable a user the connector sets the `Check Password` user attribute to `Lockout ID`.

When you disable a user account, the 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.

## 2.3.6 Creating the IT Resource for the Connector Server

To create the IT resource for the Connector Server:

1. Log in to the Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced**.
3. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.
4. On the Step 1: Provide IT Resource Information page, perform the following steps:
  - **IT Resource Name:** Enter a name for the IT resource.

- **IT Resource Type:** Select **Connector Server** from the IT Resource Type list.
  - **Remote Manager:** Do not enter a value in this field.
5. Click **Continue**. [Figure 2-6](#) shows the IT resource values added on the Create IT Resource page.

**Figure 2-6 Step 1: Provide IT Resource Information**

**Create IT Resource**

1 2 3 4 5 6

**Step 1 : Provide IT Resource Information**

Specify the IT resource name, and select the IT resource type. If the IT resource is to be accessed using a remote manager, then select a remote manager.

\* Indicates Required Field

IT Resource Name \* ConnectorServer

IT Resource Type \* Connector Server Clear

Remote Manager Clear

Cancel Continue >>

6. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. [Figure 2-7](#) shows the Step 2: Specify IT Resource Parameter Values page.

**Figure 2-7 Step 2: Specify IT Resource Parameter Values**

**Create IT Resource**

1 2 3 4 5 6

**Step 2 : Specify IT Resource Parameter Values**

Specify values for the parameters of **ConnectorServer**.

| Parameter | Value         |
|-----------|---------------|
| Host      | 172.20.45.110 |
| Key       | .....         |
| Port      | 8759          |
| Timeout   | 0             |
| UseSSL    | false         |

Cancel << Back Continue >>

[Table 2-5](#) provides information about the parameters of the IT resource.

**Table 2-5 Parameters of the IT Resource for the Connector Server**

| Parameter | Description   |
|-----------|---|
| Host      | Enter the host name or IP address of the computer hosting the connector server.<br>Sample value: RManager   |
| Key       | Enter the key for the Java connector server.  |
| Port      | Enter the number of the port at which the connector server is listening.<br>Default value: 8759   |
| Timeout   | Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out.<br>Sample value: 300   |
| UseSSL    | Enter <code>true</code> to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter <code>false</code> .<br>Default value: <code>false</code><br><b>Note:</b> It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, run the connector server by using the <code>/setKey [key]</code> option. The value of this key must be specified as the value of the Key IT resource parameter of the connector server. |

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

 **Note:**

This step is optional.

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

- a. Click **Assign Group**.
  - b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.
  - c. Click **Assign**.
8. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

 **Note:**

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

- a. Click **Update Permissions**.
  - b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.
  - c. Click **Update**.
9. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

 **Note:**

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

- a. Select the **Unassign** check box for the group that you want to unassign.
  - b. Click **Unassign**.
10. Click **Continue**. [Figure 2-8](#) shows the Step 3: Set Access Permission to IT Resource page.



Figure 2-8 Step 3: Set Access Permission to IT Resource

Create IT Resource

1 2 3 4 5 6

Step 3 : Set Access Permission to IT Resource

Specify the Administrative roles and permissions for **ConnectorServer**.

Results 1-10 of 19 First | Previous | Next | Last

| Administrative Role                      | Display Name                             | Read Access | Write Access | Delete Access | Unassign                 |
|--|--|-------------|--------------|---------------|--------------------------|
| SYSTEM ADMINISTRATORS                    | SYSTEM ADMINISTRATORS                    | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| IDENTITY USER ADMINISTRATORS             | IDENTITY USER ADMINISTRATORS             | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| ROLE ADMINISTRATORS                      | ROLE ADMINISTRATORS                      | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| REQUEST ADMINISTRATORS                   | REQUEST ADMINISTRATORS                   | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| RECONCILIATION ADMINISTRATORS            | RECONCILIATION ADMINISTRATORS            | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| ATTESTATION EVENT ADMINISTRATORS         | ATTESTATION EVENT ADMINISTRATORS         | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| APPROVAL POLICY ADMINISTRATORS           | APPROVAL POLICY ADMINISTRATORS           | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| ATTESTATION CONFIGURATION ADMINISTRATORS | ATTESTATION CONFIGURATION ADMINISTRATORS | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| USER CONFIGURATION ADMINISTRATORS        | USER CONFIGURATION ADMINISTRATORS        | ✓           | ✓            | ✓             | <input type="checkbox"/> |
| RESOURCE ADMINISTRATORS                  | RESOURCE ADMINISTRATORS                  | ✓           | ✓            | ✓             | <input type="checkbox"/> |

Unassign

First | Previous | Next | Last

Assign Role Update Permissions

Cancel << Back Continue >>

- On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.
- To proceed with the creation of the IT resource, click **Continue**. Figure 2-9 shows Step 4: Verify IT Resource Details page.

Figure 2-9 Step 4: Verify IT Resource Details

Create IT Resource 1 2 3 4 5 6

**Step 4 : Verify IT Resource Details**

Review and then submit the information that you provided. If required, use the Back button to revisit and modify information provided on the previous pages.

IT Resource Name ConnectorServer  
IT Resource Type Connector Server

| Parameter | Value         |
|-----------|---------------|
| Host      | 172.20.45.110 |
| Key       | *****         |
| Port      | 8759          |
| Timeout   | 0             |
| UseSSL    | false         |

| Administrative Role                      | Read Access | Write Access | Delete Access |
|--|-------------|--------------|---------------|
| SYSTEM ADMINISTRATORS                    | ✓           | ✓            | ✓             |
| IDENTITY USER ADMINISTRATORS             | ✓           | ✓            | ✓             |
| ROLE ADMINISTRATORS                      | ✓           | ✓            | ✓             |
| REQUEST ADMINISTRATORS                   | ✓           | ✓            | ✓             |
| RECONCILIATION ADMINISTRATORS            | ✓           | ✓            | ✓             |
| ATTESTATION EVENT ADMINISTRATORS         | ✓           | ✓            | ✓             |
| APPROVAL POLICY ADMINISTRATORS           | ✓           | ✓            | ✓             |
| ATTESTATION CONFIGURATION ADMINISTRATORS | ✓           | ✓            | ✓             |
| USER CONFIGURATION ADMINISTRATORS        | ✓           | ✓            | ✓             |
| RESOURCE ADMINISTRATORS                  | ✓           | ✓            | ✓             |
| REQUEST TEMPLATE ADMINISTRATORS          | ✓           | ✓            | ✓             |
| SCHEDULER ADMINISTRATORS                 | ✓           | ✓            | ✓             |
| NOTIFICATION TEMPLATE ADMINISTRATORS     | ✓           | ✓            | ✓             |
| SYSTEM CONFIGURATION ADMINISTRATORS      | ✓           | ✓            | ✓             |
| DEPLOYMENT MANAGER ADMINISTRATORS        | ✓           | ✓            | ✓             |
| PLUGIN ADMINISTRATORS                    | ✓           | ✓            | ✓             |
| SPML_App_Role                            | ✓           | ✓            | ✓             |
| SOD ADMINISTRATORS                       | ✓           | ✓            | ✓             |
| USER NAME ADMINISTRATORS                 | ✓           | ✓            | ✓             |

Before advancing to the next step, perform any manual steps required to connect to this IT resource. Otherwise, the target connectivity test may fail.

13. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:
- Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
  - Click **Cancel** to stop the procedure, and then begin from the first step onward.
- Figure 2-10 shows the Step 5: IT Resource Connection Result page.

**Figure 2-10 Step 5: IT Resource Connection Result**

1 2 3 4 5 6

**Step 5 : IT Resource Connection Result**

Test connectivity is not supported for the IT resource type **Connector Server**.

|         |   |               |
|---------|---|---------------|
| Host    | : | 172.20.45.110 |
| Key     | : | *****         |
| Port    | : | 8759          |
| Timeout | : | 0             |
| UseSSL  | : | false         |

Cancel << Back Continue >>

14. Click **Finish**. [Figure 2-11](#) shows the IT Resource Created Page.

Figure 2-11 Step 6: IT Resource Created

Create IT Resource

1 2 3 4 5 6

**Step 6 : IT Resource Created**

You have created **ConnectorServer**.

IT Resource Name ConnectorServer  
IT Resource Type Connector Server

| Parameter | Value         |
|-----------|---------------|
| Host      | 172.20.45.110 |
| Key       | *****         |
| Port      | 8759          |
| Timeout   | 0             |
| UseSSL    | false         |

| Administrative Role                      | Read Access | Write Access | Delete Access |
|--|-------------|--------------|---------------|
| SYSTEM ADMINISTRATORS                    | ✓           | ✓            | ✓             |
| IDENTITY USER ADMINISTRATORS             | ✓           | ✓            | ✓             |
| ROLE ADMINISTRATORS                      | ✓           | ✓            | ✓             |
| REQUEST ADMINISTRATORS                   | ✓           | ✓            | ✓             |
| RECONCILIATION ADMINISTRATORS            | ✓           | ✓            | ✓             |
| ATTESTATION EVENT ADMINISTRATORS         | ✓           | ✓            | ✓             |
| APPROVAL POLICY ADMINISTRATORS           | ✓           | ✓            | ✓             |
| ATTESTATION CONFIGURATION ADMINISTRATORS | ✓           | ✓            | ✓             |
| USER CONFIGURATION ADMINISTRATORS        | ✓           | ✓            | ✓             |
| RESOURCE ADMINISTRATORS                  | ✓           | ✓            | ✓             |
| REQUEST TEMPLATE ADMINISTRATORS          | ✓           | ✓            | ✓             |
| SCHEDULER ADMINISTRATORS                 | ✓           | ✓            | ✓             |
| NOTIFICATION TEMPLATE ADMINISTRATORS     | ✓           | ✓            | ✓             |
| SYSTEM CONFIGURATION ADMINISTRATORS      | ✓           | ✓            | ✓             |
| DEPLOYMENT MANAGER ADMINISTRATORS        | ✓           | ✓            | ✓             |
| PLUGIN ADMINISTRATORS                    | ✓           | ✓            | ✓             |
| SPML_App_Role                            | ✓           | ✓            | ✓             |
| SOD ADMINISTRATORS                       | ✓           | ✓            | ✓             |
| USER NAME ADMINISTRATORS                 | ✓           | ✓            | ✓             |

Finish

## 2.4 Upgrading the Connector

If you need to upgrade the OIM Lotus Notes/Domino connector from earlier versions to version Release 11.1.1.6.0, see *Upgrading Connectors in Oracle Fusion Middleware Administering Oracle Identity Manager* for instructions.

### Note:

For 11g R2 or later, a new UI form has to be created to see the upgraded fields. For steps to create a new UI form, follow post install section. After the creating the new UI form, modify the existing Application Instance with newly created UI form.

You can perform the upgrade process while in production, and with no downtime. Your customizations will remain intact and the upgrade should be transparent to your users.

**Note:**

During upgrade, you must keep the Trusted objects (resource object and process) as unmapped (map it to `None`).

## 2.5 Defining a Connector

You can use the Administrative and User Console to define a customized or reconfigured connector. Defining a connector is equivalent to registering the connector with Oracle Identity Manager.

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

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

When you define a connector, the following events take place:

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

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

# 3

## Using the Connector

You can use the connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.

This chapter is divided into the following sections:

- [Performing First-Time Reconciliation](#)
- [Scheduled Job for Lookup Field Synchronization](#)
- [Configuring Reconciliation](#)
- [Configuring Scheduled Jobs](#)
- [Action Scripts](#)
- [Configuring Provisioning in Oracle Identity Manager Release 11.1.2.x](#)
- [Guidelines for Performing Provisioning](#)
- [Performing Provisioning Operations on Oracle Identity Manager Release 11.1.1.x](#)
- [Switching Between Request-Based Provisioning and Direct Provisioning](#)
- [Guidelines for Performing Reconciliation](#)
- [Uninstalling the Connector](#)

### 3.1 Performing First-Time Reconciliation

After deploying the connector, you must then reconcile all existing target system user records into Oracle Identity Manager.

If you are using the target system as a trusted source, then you must configure and run the Domino Connector Trusted User Reconciliation scheduled job to reconcile user records from the target system.

 **Note:**

- See [Scheduled Jobs for Reconciliation of User Records](#) for information about the attributes for this scheduled job.
- See [Configuring Scheduled Jobs](#) for information about configuring scheduled jobs.

Reconciled user records are converted into OIM Users.

### 3.2 Scheduled Job for Lookup Field Synchronization

The Domino Connector Lookup Reconciliation scheduled job is used for lookup field synchronization.

Table 3-1 describes the attributes of this scheduled job. The procedure to configure scheduled jobs is described later in the guide.



**Note:**

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

**Table 3-1 Attributes of the Domino Connector Lookup Reconciliation Scheduled Job**

| Attribute          | Description   |
|--------------------|---|
| IT Resource Name   | Enter the name of the IT resource instance that the connector must use to reconcile data.<br>Default value: None  |
| Object Type        | Enter the Object Type you want to reconcile.<br>Default value: Group  |
| Lookup Name        | Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system.<br>Default value: Lookup.Domino.Group |
| Code Key Attribute | Enter the name of the attribute to be saved into the Code Key lookup value.<br>Default value: ListName  |
| Decode Attribute   | Enter the name of the attribute to be saved into the Decode lookup value.<br>Default value: DisplayName   |
| Filter             | Enter a filter to filter out the records to be stored in the lookup.<br>For more information and proper syntax, see " <a href="#">Performing Limited Reconciliation</a> ".  |

## 3.3 Configuring Reconciliation

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

- [Performing Full Reconciliation and Incremental Reconciliation](#)
- [Performing Limited Reconciliation](#)
- [Reconciliation Scheduled Jobs](#)

### 3.3.1 Performing Full Reconciliation and Incremental Reconciliation

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

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

1. Ensure the `Latest Token` parameter is not set. You must leave this parameter empty.

## 2. Run the Domino Connector User Reconciliation job.

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

### 3.3.2 Performing Limited Reconciliation

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

The connector provides a `Filter` parameter that allows you to use any of the Domino resource attributes to filter the target system records. (The filter is no longer restricted to four attributes, as it was in earlier releases).

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

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

While deploying the connector, follow the instructions in [Configuring Scheduled Jobs](#) to specify attribute values.

### 3.3.3 Reconciliation Scheduled Jobs

When you run the Connector Installer, reconciliation scheduled tasks are automatically created in Oracle Identity Manager.

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

#### Note:

See [Configuring Scheduled Jobs](#) for the procedure.

- [Scheduled Jobs for Reconciliation of User Records](#)
- [Scheduled Jobs for Reconciliation of Deleted Users](#)

#### 3.3.3.1 Scheduled Jobs for Reconciliation of User Records

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

- Domino Connector User Reconciliation (scheduled job for target resource reconciliation)
- Domino Connector Trusted User Reconciliation (scheduled job for trusted source reconciliation)



Table 3-2 describes the attributes of both scheduled jobs.

**Table 3-2 Attributes of the Scheduled Jobs for Reconciliation of User Records**

| Attribute                        | Description   |
|----------------------------------|---|
| IT Resource Name                 | Name of the IT resource instance that the connector must use to reconcile data.<br>Default is: None   |
| Resource Object Name             | Name of the resource object.<br>Default is: Lotus User for target resource reconciliation or Lotus Trusted User for trusted source reconciliation.  |
| Object Type                      | Object Type to be reconciled.<br>Default is: User   |
| Filter                           | Expression for filtering records. Use the following syntax:<br><br><pre>syntax = expression ( operator expression )* operator = 'and'   'or' expression = ( 'not' )? filter filter = ('equalTo'   'contains'   'containsAllValues'   'startsWith'   'endsWith'   'greaterThan'   'greaterThanOrEqualTo'   'lessThan'   'lessThanOrEqualTo' ) '(' 'attributeName' ',' attributeValue ')'</pre> attributeValue = singleValue   multipleValues<br>singleValue = 'value'<br>multipleValues = '[' 'value_1' (',' 'value_n')* ']'<br><br>Default is: None |
| Latest Token                     | Latest Date the reconciliation was run.<br>Default is: None   |
| Incremental Recon Date Attribute | Domino Attribute used to get the object's modification date.<br>Default is: LastModified  |

### 3.3.3.2 Scheduled Jobs for Reconciliation of Deleted Users

Table 3-3 describes the attributes of the Domino Connector Delete Reconciliation scheduled job for reconciliation of deleted users.

**Table 3-3 Attributes of the Domino Connector Delete Reconciliation Scheduled Job**

| Attribute            | Description   |
|----------------------|---|
| IT Resource Name     | Name of the IT resource instance that the connector must use to reconcile data.<br>Default is: None |
| Resource Object Name | Name of the resource object.<br>Default is: Lotus User  |
| Object Type          | Object Type to be reconciled.<br>Default is: User   |

**Table 3-3 (Cont.) Attributes of the Domino Connector Delete Reconciliation Scheduled Job**

| Attribute | Description  |
|-----------|--|
| Filter    | <p>Expression for filtering records. Use the following syntax:</p> <pre> syntax = expression ( operator expression )* operator = 'and'   'or' expression = ( 'not' )? filter filter = ('equalTo'   'contains'   'containsAllValues'   'startsWith'   'endsWith'   'greaterThan'   'greaterThanOrEqualTo'   'lessThan'   'lessThanOrEqualTo' ) '(' 'attributeName' ',' attributeValue ') attributeValue = singleValue   multipleValues singleValue = 'value' multipleValues = '[' 'value_1' (',' 'value_n')* ']'                     </pre> <p>Default is: None</p> |

Table 3-4 describes the attributes of the Domino Connector Trusted Delete Reconciliation scheduled job for the trusted reconciliation of deleted users.

**Table 3-4 Attributes of the Domino Connector Trusted Delete Reconciliation Scheduled Job**

| Attribute                | Description   |
|--------------------------|---|
| Trusted IT Resource Name | <p>Name of the trusted IT resource instance that the connector must use to reconcile data.</p> <p>Default is: None</p>  |
| Resource Object Name     | <p>Name of the resource object.</p> <p>Default is: Lotus Trusted User</p>   |
| Object Type              | <p>Object Type to be reconciled.</p> <p>Default is: User</p>  |
| Filter                   | <p>Expression for filtering records. Use the following syntax:</p> <pre> syntax = expression ( operator expression )* operator = 'and'   'or' expression = ( 'not' )? filter filter = ('equalTo'   'contains'   'containsAllValues'   'startsWith'   'endsWith'   'greaterThan'   'greaterThanOrEqualTo'   'lessThan'   'lessThanOrEqualTo' )  '(' 'attributeName' ',' attributeValue ') attributeValue = singleValue   multipleValues singleValue = 'value' multipleValues = '[' 'value_1' (',' 'value_n')* ']'                     </pre> <p>Default is: None</p> |

## 3.4 Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Table 3-5 lists the scheduled jobs shipped as part of the connector.

**Table 3-5 Scheduled Jobs for Lookup Field Synchronization and Reconciliation**

| Scheduled Job                                  | Description   |
|--|---|
| Domino Connector Lookup Reconciliation         | This scheduled job is used for lookup field synchronization.                                  |
| Domino Connector User Reconciliation           | This scheduled job is used for user reconciliation in target resource mode.                   |
| Domino Connector Trusted User Reconciliation   | This scheduled job is used for user reconciliation in trusted source mode.                    |
| Domino Connector Delete Reconciliation         | This scheduled job is used for reconciliation of deleted user records.                        |
| Domino Connector Trusted Delete Reconciliation | This scheduled job is used for reconciliation of deleted user records in trusted source mode. |

## 3.5 Configuring Scheduled Jobs

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

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1:
  - a. Log in to the Administrative and User Console.
  - b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
  - c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
2. If you are using Oracle Identity Manager release 11.1.2.x:
  - a. Log in to Oracle Identity System Administration.
  - b. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the scheduled job as follows:
  - a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
  - b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
  - c. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. On the Job Details tab, you can modify the following parameters:
  - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.
  - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

 **Note:**

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

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

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

 **Note:**

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) can be left empty.
- Attributes of the scheduled job are discussed in [Reconciliation Scheduled Jobs](#).

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

6. After specifying the attributes, click **Apply** to save the changes.

 **Note:**

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

## 3.6 Action Scripts

 **Note:**

Action Scripts on 11gR2 works only on OIM version 11.1.1.5.8 or later.

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

The following sections provide information related to action scripts:

- [Understanding Action Scripts](#)
- [Configuration Examples](#)

- [Accessing Variables from Script](#)
- [Configuring Action Scripts](#)

 **Note:**

- Script on connector is supported on windows machines only.
- To configure a before or after action, your connector must support running scripts. An exception is Groovy (with target set to **Connector**), which the Identity Connector Framework (ICF) supports by default for all converged connectors.

## 3.6.1 Understanding Action Scripts

The IBM Lotus Notes and Domino connector supports

- **CMD**: windows batch script and **target**: Connector
- **lotusscript**: Lotus Script and **target**: Resource

The target means where the script is executed.

- If the target is *Connector*, then the script is executed on the same computer where the connector is deployed. For example, if you deploy the connector on the connector server, the script will be executed on that computer.
- If the target is *Resource*, then the script is executed on the computer where the target resource is running (on Lotus Domino Server in this case).

Both the scripts when executed have access to form fields via variables, CMD can use environment variables and LOTUSSCRIPT can use DocumentContext to get the variable value. The variables have WSUSER\_ prefix for every variable which was provided as part of the script execution.

In addition, Oracle Identity Manager can be configured to provide script options. Script options can be configured in two way: Operation Options Mapping, which is form field mapping common for all scripts per object type and Action Options which is static string settings per action. These script options are available to scripts, the same as the form fields (via variables).

 **Note:**

To execute lotusscript with Domino Connector, the following two options need to be provided either as part of Operation Options Mapping or Action Mappings (recommended way):

- **agentName** – with value specifies the name of the agent created on Domino Server, for example, oim-script.
- **agentCreate** – this value specifies if an agent should be created (if doesn't exist) on Domino Server, the recommended value is "true"

The actions (script execution) can be configured in Oracle Identity Manager before or after the following provisioning events:

- create
- update
- delete

[Table 3-6](#) shows here what is provided by ICF-INTG to the connector when executing an action:

**Table 3-6 Output by ICF-INTG**

| Operation | Form fields   | Operation Options Mapping    | Action Options                |
|-----------|---|------------------------------|-------------------------------|
| Create    | All form fields provided to create operation          | All mapped fields configured | All action options configured |
| Update    | Form fields which were updated<br><b>Note:</b> no uid | All mapped fields configured | All action options configured |
| Delete    | Uid only  | All mapped fields configured | All action options configured |

## 3.6.2 Configuration Examples

This section provides example configurations for configuring action scripts.

### Example 1 of Configuration

In this example, Oracle Identity Manager is configured to run script.bat for every (create/update/delete) domino provisioning operation as shown in [Figure 3-1](#):

Figure 3-1 Lookup Domino Configuration

**Lookup Definition**

Code

Field

Lookup Type  Field Type

Required

Group

---

**Lookup Code Information**

| Add | Code Key ▼                      | Decode                        |
|-----|---------------------------------|-------------------------------|
|     | 1 Before Create Action File     | /space/tknappek/script.bat    |
|     | 2 Before Create Action Language | cmd                           |
|     | 3 Before Create Action Target   | connector                     |
|     | 4 Before Delete Action File     | /space/tknappek/script.bat    |
|     | 5 Before Delete Action Language | cmd                           |
|     | 6 Before Delete Action Target   | connector                     |
|     | 7 Before Update Action File     | /space/tknappek/script.bat    |
|     | 8 Before Update Action Language | cmd                           |
|     | 9 Before Update Action Target   | connector                     |
|     | 10 Provisioning Attribute Map   | Lookup.Domino.UM.ProvAttrMap  |
|     | 11 Recon Attribute Map          | Lookup.Domino.UM.ReconAttrMap |

Script.bat file:

```
set >c:\script.out
```

When a provisioning operation is performed then the action is executed and script.out will have the following content:

**Create Operation:**

```
WSUSER_accountId=test otest03191
WSUSER_Comment="some comment"
WSUSER_EndDate=0
WSUSER_FirstName=test
WSUSER_idFile=f:\otest03191.id
WSUSER_LastName=otest03191
WSUSER_MailFile=mail/otest03191.nsf
WSUSER_MoveCertifier=false
WSUSER_NorthAmerican=false
WSUSER_Recertify=false
WSUSER_ShortName=otest03191
WSUSER__PASSWORD_=org.identityconnectors.common.security.GuardedString@e3259c99
```

Update Operation (update of one field):

```
WSUSER_Comment="some comment updated"
```

Update Operation (update of multiple fields):

```
WSUSER_Comment="comment updated"
WSUSER_Location="location updated"
WSUSER__CURRENT_ATTRIBUTES__="{Attributes=[Attribute: {Name=Recertify,
```

```
Value=[false]}, Attribute: {Name=idFile, Value=[f:\otest03191.id]}, Attribute:
{Name=NorthAmerican, Value=[false]}, Attribute: {Name=MailFile, Value=[mail/
otest03191.nsf]}, Attribute: {Name=FirstName, Value=[test]}, Attribute:
{Name=MoveCertifier, Value=[false]}, Attribute: {Name=Comment, Value=[some comment
updated]}, Attribute: {Name=__NAME__, Value=[test otest03191]}, Attribute:
{Name=ShortName, Value=[otest03191]}, Attribute: {Name=__PASSWORD__,
Value=[org.identityconnectors.common.security.GuardedString@e3259c99]}, Attribute:
{Name=LastName, Value=[otest03191]}, Attribute: {Name=EndDate, Value=[0]},
ObjectClass=ObjectClass: __ACCOUNT__}"
```

Delete Operation:

```
WSUSER_UNID=A3F0AE57AD341B0D80257B3300766FCF
```

Example 2 of Configuration:

You can configure the operations options mapping to provide, for example, First Name, Last Name, and Universal Id by the following steps:

1. Create a lookup with value as shown in [Figure 3-2](#):

**Figure 3-2 Creating Lookup**

**Lookup Definition**

Code:

Field:

Lookup Type  Field Type

Required:

Group:

**Lookup Code Information**

|                                       | Code Key ▼     |           |
|---------------------------------------|----------------|-----------|
| <input type="button" value="Add"/>    | 1 First Name   | FirstName |
| <input type="button" value="Delete"/> | 2 Last Name    | LastName  |
|                                       | 3 Universal Id | UNID      |

2. Link this lookup to the original object type configuration as shown in [Figure 3-3](#):



Figure 3-3 Linking Lookup

**Lookup Definition**

Code

Field

Lookup Type  Field Type

Required

Group

---

**Lookup Code Information**

|                                       | Code Key ▼                      | Decode                        |
|---------------------------------------|---------------------------------|-------------------------------|
| <input type="button" value="Add"/>    | 1 Before Create Action File     | /space/tknappek/script.bat    |
| <input type="button" value="Delete"/> | 2 Before Create Action Language | cmd                           |
|                                       | 3 Before Create Action Target   | connector                     |
|                                       | 4 Before Delete Action File     | /space/tknappek/script.bat    |
|                                       | 5 Before Delete Action Language | cmd                           |
|                                       | 6 Before Delete Action Target   | connector                     |
|                                       | 7 Before Update Action File     | /space/tknappek/script.bat    |
|                                       | 8 Before Update Action Language | cmd                           |
|                                       | 9 Before Update Action Target   | connector                     |
|                                       | 10 Operation Options Map        | Lookup.Domino.UM.OptionsMap1  |
|                                       | 11 Provisioning Attribute Map   | Lookup.Domino.UM.ProvAttrMap  |
|                                       | 12 Recon Attribute Map          | Lookup.Domino.UM.ReconAttrMap |

3. Leave script.bat unchanged.
4. When a provisioning operation is performed then the action is executed and script.out will have the following content:

**Create Operation:**

```

WSUSER_accountId=test otest03192
WSUSER_Comment="some comment"
WSUSER_EndDate=0
WSUSER_FirstName=test
WSUSER_idFile=f:/otest03192.id
WSUSER_LastName=otest03192
WSUSER_MailFile=mail/otest03192.nsf
WSUSER_MoveCertifier=false
WSUSER_NorthAmerican=false
WSUSER_Recertify=false
WSUSER_ShortName=otest03192
WSUSER__PASSWORD__=org.identityconnectors.common.security.GuardedString@e3259c99

```

**Update Operation (update of one field):**

```

WSUSER_Comment="some comment updated"
WSUSER_FirstName=test
WSUSER_LastName=otest03192
WSUSER_UNID=3B97A9C002AF3B2580257B330079E757

```

**Update Operation (update of multiple field):**

```

WSUSER_Comment="comment updated"
WSUSER_FirstName=test
WSUSER_LastName=otest03192

```

```
WSUSER_Location="location updated"
WSUSER_UNID=3B97A9C002AF3B2580257B330079E757
WSUSER__CURRENT_ATTRIBUTES__="{Attributes=[Attribute: {Name=Recertify,
Value=[false]}, Attribute: {Name=idFile, Value=[f:/otest03192.id]}, Attribute:
{Name=NorthAmerican, Value=[false]}, Attribute: {Name=MailFile, Value=[mail/
otest03192.nsf]}, Attribute: {Name=FirstName, Value=[test]}, Attribute:
{Name=MoveCertifier, Value=[false]}, Attribute: {Name=Comment, Value=[some comment
updated]}, Attribute: {Name=__NAME__, Value=[test otest03192]}, Attribute:
{Name=ShortName, Value=[otest03192]}, Attribute: {Name=__PASSWORD__,
Value=[org.identityconnectors.common.security.GuardedString@e3259c99]}, Attribute:
{Name=LastName, Value=[otest03192]}, Attribute: {Name=EndDate, Value=[0]}],
ObjectClass=ObjectClass: __ACCOUNT__}"
```

#### Delete Operation:

```
SUSER_FirstName=test
WSUSER_LastName=otest03192
WSUSER_UNID=3B97A9C002AF3B2580257B330079E757
```

#### Example 3 of Configuration:

Keep the existing configuration from Example 2 and add Action Options for each action (create/update/delete). You can configure the same Action options for all of them, but each action can have different options.

Figure 3-4 and Figure 3-5 shows one action option configured:

Figure 3-4 Linking Lookup

**Lookup Definition**

Code

Field

Lookup Type  Field Type

Required

Group

---

**Lookup Code Information**

|                                       | Code Key ▼                       | Decode                         |
|---------------------------------------|----------------------------------|--------------------------------|
| <input type="button" value="Add"/>    | 1 Before Create Action File      | /space/tknappek/script.bat     |
| <input type="button" value="Delete"/> | 2 Before Create Action Language  | cmd                            |
|                                       | 3 Before Create Action Options   | Lookup.Domino.UM.ActionOptions |
|                                       | 4 Before Create Action Target    | connector                      |
|                                       | 5 Before Delete Action File      | /space/tknappek/script.bat     |
|                                       | 6 Before Delete Action Language  | cmd                            |
|                                       | 7 Before Delete Action Options   | Lookup.Domino.UM.ActionOptions |
|                                       | 8 Before Delete Action Target    | connector                      |
|                                       | 9 Before Update Action File      | /space/tknappek/script.bat     |
|                                       | 10 Before Update Action Language | cmd                            |
|                                       | 11 Before Update Action Options  | Lookup.Domino.UM.ActionOptions |
|                                       | 12 Before Update Action Target   | connector                      |
|                                       | 13 Operation Options Map         | Lookup.Domino.UM.OptionsMap1   |
|                                       | 14 Provisioning Attribute Map    | Lookup.Domino.UM.ProvAttrMap   |
|                                       | 15 Recon Attribute Map           | Lookup.Domino.UM.ReconAttrMap  |

Figure 3-5 Configuring Lookup

**Lookup Definition**

Code

Field

Lookup Type  Field Type

Required

Group

---

**Lookup Code Information**

|   | Code Key ▼         | Decode                  |
|---|--------------------|-------------------------|
| 1 | CustomActionOption | CustomActionOptionValue |

When a provisioning operation is performed then the action is executed and script.out will have the following content:

**Create Operation:**

```
WSUSER_accountId=test otest03193
WSUSER_Comment="some comment"
WSUSER_CustomActionOption=CustomActionOptionValue
WSUSER_EndDate=0
WSUSER_FirstName=test
WSUSER_idFile=f:\otest03193.id
WSUSER_LastName=otest03193
WSUSER_MailFile=mail/otest03193.nsf
WSUSER_MoveCertifier=false
WSUSER_NorthAmerican=false
WSUSER_Recertify=false
WSUSER_ShortName=otest03193
WSUSER__PASSWORD__=org.identityconnectors.common.security.GuardedString@e3259c99
```

**Update Operation (update of one field):**

```
WSUSER_Comment="some comment updated"
WSUSER_CustomActionOption=CustomActionOptionValue
WSUSER_FirstName=test
WSUSER_LastName=otest03193
WSUSER_UNID=885A2EBA9F6C4F9680257B33007BF3A6
```

**Update Operation (update of multiple fields):**

```
WSUSER_Comment="comment updated"
WSUSER_CustomActionOption=CustomActionOptionValue
WSUSER_FirstName=test
WSUSER_LastName=otest03193
WSUSER_Location="location updated"
```

```
WSUSER_UNID=885A2EBA9F6C4F9680257B33007BF3A6
WSUSER__CURRENT_ATTRIBUTES__="{Attributes=[Attribute: {Name=Recertify,
Value=[false]}, Attribute: {Name=idFile, Value=[f:\otest03193.id]}, Attribute:
{Name=NorthAmerican, Value=[false]}, Attribute: {Name=MailFile, Value=[mail/
otest03193.nsf]}, Attribute: {Name=FirstName, Value=[test]}, Attribute:
{Name=MoveCertifier, Value=[false]}, Attribute: {Name=Comment, Value=[some comment
updated]}, Attribute: {Name=__NAME__, Value=[test otest03193]}, Attribute:
{Name=ShortName, Value=[otest03193]}, Attribute: {Name=__PASSWORD__,
Value=[org.identityconnectors.common.security.GuardedString@e3259c99]}, Attribute:
{Name=LastName, Value=[otest03193]}, Attribute: {Name=EndDate, Value=[0]}],
ObjectClass=ObjectClass: __ACCOUNT__}"
```

### Delete Operation:

```
WSUSER_CustomActionOption=CustomActionOptionValue
WSUSER_FirstName=test
WSUSER_LastName=otest03192
WSUSER_UNID=3B97A9C002AF3B2580257B330079E757
```

## 3.6.3 Accessing Variables from Script

### CMD:

Environment variables are used, it can be accessed with %VARIABLE%.  
Example:  
echo "%WSUSER\_UNID%"

### LOTUSSCRIPT:

Domino for example:

```
Sub Initialize
  Main
End Sub
Sub Main
  Dim session As New NotesSession
  Dim doc As NotesDocument
  Set doc = session.DocumentContext
  Dim unid As Variant
  unid = doc.GetItemValue("WSUSER_UNID")
End Sub
```

## 3.6.4 Configuring Action Scripts

To configure the action:

1. Log in to the Design Console.
2. Search and open Lookup.Domino.UM.Configuration.
3. Add the following new values:
  - **Code Key:** Before Create Action Language
  - **Decode:** Enter the scripting language of the script you want to execute
  - **Example:** cmd
4. Add these new values:
  - **Code Key:** Before Create Action File

- **Decode:** Enter the full path to the file containing the script to be executed (OIM must be able to access this file.)
  - **Example:** /home/scripts/testscript.bat
5. Add these new values:
- **Code Key:** Before Create Action Target
  - **Decode:** Allowed values are `Connector` and `Resource`, depending on the connector what is supported.
- As previously stated, the IBM Lotus Notes and Domino connector supports the `CMD` script for a `Connector` target.
- **Example:** `Connector`
6. Save the lookup.

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

## 3.7 Configuring Provisioning in Oracle Identity Manager Release 11.1.2.x

To configure provisioning operations in Oracle Identity Manager release 11.1.2.x:

### Note:

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

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

## 3.8 Guidelines for Performing Provisioning

Apply the following guidelines while performing provisioning.

- You must enter values for the following mandatory attributes during provisioning operations:
  - Last Name
  - Server Name
  - Password
- The `IDFile Name` and `Mail File Name` attributes are unique for each user. The `Mail File Already Exists` error message is displayed if you enter a file name that already exists on the target system.
- If you specify `True` as the value of the `createMailDBInBackground` attribute, then the connector does not check whether mail files are successfully created during `Create User` provisioning operations.
- Password update will not work if `ID File Name` is not provided for that user while provisioning.

## 3.9 Performing Provisioning Operations on Oracle Identity Manager Release 11.1.1.x

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

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

If you configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in [Switching Between Request-Based Provisioning and Direct Provisioning](#).

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

 **Note:**

This does not apply if you are using OIM 11.1.2.x or later.

 **Note:**

Oracle Identity Manager does not indicate the status of provisioning operations. After a provisioning operation, if the connector status is

- **Provisioned**, the operation was successful.
- **Provisioning**, the operation failed.

To determine whether the problem occurred during an update or create operation, click **Resource History** for details.

 **See Also:**

Managing Provisioning Tasks in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about the types of provisioning

This section discusses the following topics:

- [Direct Provisioning](#)
- [Request-Based Provisioning](#)

## 3.9.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
  - a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.
  - b. On the Create User page, enter values for the OIM User fields, and then click **Save**.
3. If you want to provision a target system account to an existing OIM User, then:
  - a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
  - b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. On the user details page, click the **Resources** tab.
5. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
6. On the Step 1: Select a Resource page, select **Lotus Notes** from the list and then click **Continue**.
7. On the Step 2: Verify Resource Selection page, click **Continue**.



8. On the Step 5: Provide Process Data for Lotus User page, enter the details of the account that you want to create on the target system and then click **Continue**.
9. On the Step 5: Provide Process Data for Lotus User page, search for and select a group for the user on the target system and then click **Continue**.
10. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.  
The "Provisioning has been initiated" message is displayed.
11. Close the window displaying the "Provisioning has been initiated" message.
12. On the Resources tab, click **Refresh** to view the newly provisioned resource.

## 3.9.2 Request-Based Provisioning

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



### Note:

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

- [End User's Role in Request-Based Provisioning](#)
- [Approver's Role in Request-Based Provisioning](#)

### 3.9.2.1 End User's Role in Request-Based Provisioning

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

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.  
The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **Lotus User**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
  - Effective Date
  - Justification

On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

### 3.9.2.2 Approver's Role in Request-Based Provisioning

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

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

A message confirming that the task was approved is displayed.

## 3.10 Switching Between Request-Based Provisioning and Direct Provisioning

If you have configured the connector for request-based provisioning, you can always switch to direct provisioning. Similarly, you can always switch back to request-based provisioning any time. This section discusses the following topics:

- [Switching From Request-Based Provisioning to Direct Provisioning](#)
- [Switching From Direct Provisioning to Request-Based Provisioning](#)

### 3.10.1 Switching From Request-Based Provisioning to Direct Provisioning

If you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
  - a. Expand **Process Management**, and then double-click **Process Definition**.
  - b. Search for and open the **Lotus User** process definition.
  - c. Deselect the Auto Save Form check box.
  - d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
  - a. Expand **Resource Management**, and then double-click **Resource Objects**.
  - b. Search for and open the **Lotus User** resource object.
  - c. Deselect the Self Request Allowed check box.
  - d. Click the Save icon.

### 3.10.2 Switching From Direct Provisioning to Request-Based Provisioning

If you want to switch from direct provisioning back to request-based provisioning, then:

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

## 3.11 Guidelines for Performing Reconciliation

Apply the following guidelines while performing reconciliation.

Oracle Identity Manager does not fetch values for the following fields from the target system during reconciliation:

- Certifier ID File Path

- Certifier Password
- IDFile Name
- Mail Replica Servers
- Organization Unit
- Recertify
- MoveCertifier

When an account is created in Oracle Identity Manager through reconciliation of a new record from the target system, you must manually set values for these fields.

## 3.12 Uninstalling the Connector

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

# 4

## Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.

This chapter discusses the following optional procedures:

### Note:

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

- [Adding Target System Attributes for Reconciliation](#)
- [Adding Target System Attributes for Provisioning](#)
- [Configuring Validation and Transformation](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)
- [Moving the User Name in the Name Hierarchy](#)
- [Creating and Updating WebUsers](#)
- [Resetting the User Password in IDVault](#)

### 4.1 Adding Target System Attributes for Reconciliation

By default, the attributes listed in the "[User Attributes](#)" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation as follows:

### Note:

Perform this procedure only if you want to add new target system attributes for reconciliation.

1. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:
  - a. Open the Resource Objects form. This form is in the Resource Management folder.

- b. Click **Query for Records**.
  - c. On the Resource Objects Table tab, double-click the **Lotus User** resource object to open it for editing.
  - d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
  - e. Specify a value for the field name.  
You must specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 1.  
For example, if you uncomment the `Users.City=City` line in Step 1, then you must specify `Users.City` as the attribute name.
  - f. From the **Field Type** list, select a data type for the field.  
For example: `String`
  - g. Save the values that you enter, and then close the dialog box.
  - h. If required, repeat Steps d through g to map more fields.
  - i. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile**. This copies changes made to the resource object into the MDS.
2. 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 2.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**.
3. Modify the process definition to include the mapping between the newly added attribute and the corresponding reconciliation field:
    - a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.
    - b. Click the **Query for Records** icon.

- c. On the Process Definition Table tab, double-click the **Lotus User** process definition.
  - d. On the Reconciliation Field Mappings tab, click **Add Field Map** to open the Add Reconciliation Field Mapping dialog box.
  - e. From the **Field Name** list, select the name of the resource object that you add in Step 2.1.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 3.c through 3.g to map more fields.
4. Go to the reconciliation lookup, Lookup.Domino.UM.ProvAttrMap, and add a new record for the new attribute using the following values:
    - **Code Key** - Name of the reconciliation field
    - **Decode** - Name of the Domino Attribute

## 4.2 Adding Target System Attributes for Provisioning

### Note:

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

Do not repeat steps that you have performed as part of the procedure described in [Adding Target System Attributes for Reconciliation](#).

By default, the attributes listed in the "[User Attributes](#)" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning by performing these steps:

1. Add a new form field.

To add a new field to the Process form, use the following steps:

- 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 4.
- g. On the Additional Columns tab, click **Add**.
- h. Specify the new field name and other values.

- i. Click **Save**.
- j. Click **Make Version Active** to make the new form field visible to the user.

Now, if you go to Oracle Identity Manager, and try to provision a new user to Domino, you should see the new form field. Next, you must add the new form field to the Provisioning Mapping Lookup.

2. Add the new field to the Provisioning Mapping Lookup.

After creating a new form field, you must add that field to the Provisioning Mapping Lookup. Use the following steps:

- a. Expand **Administration** and then double-click **Lookup Definition**.

- b. In the Lookup Definition window, search for **\*Domino\***.

The Design Console returns Lookup.Domino.UM.ProvAttrMap.

- c. Select the Lookup Definition Table tab, and select

Lookup.Domino.UM.ProvAttrMap.

The Lookup Code Information tab maps the OIM form field names and the Domino Identity Connector attributes. Where the Code Key column contains the OIM field labels and the Decode column contains the attribute names supported by the Domino Identity Connector.

- d. Add a new record for the new form field. Type the new form field name into the Code Key column and type the Domino Identity Connector attribute name into the Decode column.

- e. Click **Save**.

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

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

3. Change the process task to handle updates by performing these steps:

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

- b. Search for, and select the **Lotus User** process.

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

- d. Click **Add**.

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

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

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

- **Conditional**: Enabled
- **Required for Completion**: Disabled
- **Disable Manual Insert**: Disabled



- **Allow Cancellation while Pending:** Enabled

- **Allow Multiple Instances:** Enabled

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

- g. Save your changes.
- h. To add an Event Handler, select the **Integration** tab, and then click **Add**.
- i. When the Handler Select dialog box displays, select **Adapter** as the handler type and then select **adpLNUPDATEUSERINFO** and click **Save**.
- j. Map all of the variables that are configured for the event adapter.

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

| Variable Name        | Map To        | Qualifier        | Literal Value                          |
|----------------------|---------------|------------------|--|
| itResourceFieldName  | Literal       | String           | UD_LOTUS_SERVERNAME                    |
| processInstanceKey   | Process Data  | Process Instance |  |
| Adapter return value | Response Code |                  |  |
| objectType           | Literal       | String           | User                                   |
| attrName             | Literal       | String           | Enter your new <i>Form Field Label</i> |

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

## 4.3 Configuring Validation and Transformation

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

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

- [Configuring Validation for Provisioning](#)
- [Configuring Validation for Reconciliation](#)
- [Configuring Reconciliation Transformation](#)

### 4.3.1 Configuring Validation for Provisioning

To configure validation for provisioned data, follow these steps:

1. Write some custom Java class code to implement the Validation interface. For example:

```

package com.validationexample;
import oracle.iam.connectors.common.ConnectorException;

import java.util.HashMap;

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

        /* You must write code to validate attributes. Parent
        * data values can be fetched by using hmUserDetails.get(field)
        * For child data values, loop through the
        * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")

        * Depending on the outcome of the validation operation,
        * the code must return true or false.
        */

        /*
        * In this sample code, the value "false" is returned if the field
        * contains the number sign (#). Otherwise, the value "true" is
        * returned.
        */
        boolean valid = true;
        String sFirstName = (String) hmUserDetails.get(sField);
        for (int i = 0; i < sFirstName.length(); i++) {
            if (sFirstName.charAt(i) == '#') {
                valid = false;
                break;
            }
        }
        return valid;
    }
}

```

2. Log into the Design Console.
3. Search for and open the **Lookup.Domino.UM.ProvValidation** (or create another custom name) lookup definition.

 **Note:**

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

4. In the **Code Key** column, enter the resource object field name that you want to validate.
5. In the **Decode** column, enter the class name.  
For example, `com.validationexample.MyValidator`.
6. Save your changes to the lookup definition.
7. Search for and open the `Lookup.Domino.UM.Configuration` lookup definition.
8. In the **Code Key** column, enter `Provisioning Validation Lookup`.
9. In the **Decode** column, enter `Lookup.Domino.UM.ProvValidation` or enter the name of the lookup you created in step 3.

## 4.3.2 Configuring Validation for Reconciliation

The steps for configuring reconciliation validation are the same as the steps described in [Configuring Validation for Provisioning](#), except that the Code Key in step 8 must be **Recon Validation Lookup**.

## 4.3.3 Configuring Reconciliation Transformation

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

To configure the reconciliation transformation:

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

```
package com.transformationexample;
import oracle.iam.connectors.common.ConnectorException;

import java.util.HashMap;

public class MyTransformer implements Transformation {
    public Object transform(HashMap hmUserDetails, HashMap hmEntitlementDetails,
String sField) throws ConnectorException {
        /*
         * You must write code to transform the attributes.
         * Parent data attribute values can be fetched by
         * using hmUserDetails.get("Field Name").
         * To fetch child data values, loop through the
         * ArrayList/Vector fetched by hmEntitlementDetails.get("Child
Table")
         * Return the transformed attribute.
         */
        String sFirstName = (String) hmUserDetails.get("First Name");
        String sLastName = (String) hmUserDetails.get("Last Name");
        return sFirstName + "." + sLastName;
    }
}
```

2. Log in to the Design Console.
3. Search for and open the `Lookup.Domino.UM.ReconTransformation` (or create another custom name) lookup definition.

 **Note:**

If you cannot find the `Lookup.Domino.UM.ReconTransformation` lookup definition, create a new lookup.

4. In the **Code Key** column, enter the resource object field name you want to transform.
5. In the **Decode** column, enter the class name.  
For example, `com.transformationexample.MyTransformer`.

6. Save the changes to the lookup definition.
7. Search for and open the **Lookup.Domino.UM.Configuration** lookup definition.
8. In the **Code Key** column, enter `Recon Transformation Lookup`.
9. In the **Decode** column, enter `Lookup.Domino.UM.ReconTransformation` or enter the name of the lookup you created in step 3.

## 4.4 Configuring the Connector for Multiple Installations of the Target System



### Note:

Perform this procedure only if you want to configure the connector for multiple installations of IBM Lotus Notes and Domino.

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

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

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

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

To create copies of the connector objects:



### Note:

For this connector, it is assumed that all installation of the target system have the same set of attributes for reconciliation and provisioning.

1. Create a copy of the IT resource. See "[Configuring the IT Resource](#)" for information about this IT resource.
2. Create a copy of the Lotus Notes User Reconciliation scheduled job. See "[Reconciliation Scheduled Jobs](#)" for information about this scheduled job.

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

## 4.5 Moving the User Name in the Name Hierarchy

If you want to move the username in the name hierarchy then perform the following steps.

1. Change the **CertifierOrgHierarchy** with new org info (example: org2/org) in the process form.
2. Give the values of new **certifier id path** and **certpassword** in the process form.
3. Check the **movecertifier** checkbox.
4. Click **Save**.

### Note:

To make the above feature work, you should copy the root certificate, current certificate, and the certificate that you are moving into the "Servers\Certificates" view of the inbound domain's Name and Address book (Domino Directory). You can also create the documents if you have the Certifier ID files.

## 4.6 Creating and Updating WebUsers

If you want to create and update WebUsers, perform the following procedure:

### Note:

The following procedure is applicable only for WebUsers.

1. To create a WebUser in Domino, set the configuration option of CreateIdFile as false in the Lookup.Configuration.Domino lookup definition. To do so, perform the following procedure:
  - a. Log into the Design Console.
  - b. Search for and open the **Lookup.Configuration.Domino** lookup definition.
  - c. Set the configuration option of CreateIdFile to `False`.
  - d. Click **Save** and close the lookup definition.
2. While provisioning, enter the cert org hierarchy value in the process form in order to ensure that the WebUsers Update functionality works as expected.

## 4.7 Resetting the User Password in IDVault

This connector supports the reset password functionality in the idvault. To achieve this you need to set the useIDVault to be true in the Lookup.Configuration.Domino.

On the target side "The IDVault can be configured for certain organization or can use policy to decide if the IDFile should be stored in IDVault. Also Domino Connector support using explicit policy when registering new user."

# 5


## Testing and Troubleshooting

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

- [Testing the Connector](#)
- [Troubleshooting](#)

### 5.1 Testing the Connector

You can use the testing utility, supplied with the OIM Lotus Notes/Domino Connector package, to test basic provisioning operations (create, update, or delete) on a configurable target resource. The testing utility is implemented using ICF to invoke connector operations on the Domino Identity Connector, which is an approach that is quite similar to a Domino Connector deployed in OIM. You can configure the testing utility to use the connector server.

 **Note:**

Before running the testing utility, you must place Notes.jar files in `JAVA_HOME/jre/lib/ext` or with `classpath`.

To use the testing utility, perform the following steps:

1. Set the `CLASSPATH` variable to contain the following jars:
  - `connector-framework.jar`
  - `connector-framework-internal.jar`
  - `groovy-all.jar`

 **Note:**

These files are delivered as part of the OIM EAR application, and they are located in the `oim.ear/APP-INF/lib` directory.

You must add these three jar files to the `JAVA_HOME/jre/lib/ext` folder to run the test utility.

2. Unzip the OIM Domino Connector zip file.
3. Locate the `test-utility` directory.
4. Update the `example-config.groovy` file to reflect your local settings. The `example-config.groovy` file contains the following content:

```
>>>> example-config.groovy >>>>>>>
import org.identityconnectors.common.security.GuardedString

// ICF Configuration
icf {
    bundleName = 'org.identityconnectors.domino'
    bundleVersion = '2.0.1'
    connectorName = 'org.identityconnectors.domino.DominoConnector'
    //bundle = ''
    // Configure your connector server instance
    connectorServer {
        host = 'myhost'
        port = 8759
        key = 'mykey'
    }
}

// Connector Configuration - update with your environment information
connector {
    adminIdFile = 'c:\\Notes85\\Data\\user.id'
    adminName = 'administrator/ACME'
    adminPassword = new GuardedString('changeit'.toCharArray())
    administrationServer = 'myreg.server.example.com'
    certifierIdFile = 'c:\\data\\cert.id'
    certifierPassword = new GuardedString('changeit'.toCharArray())
    createIdFile = true
    createMailDB = false
    registrationServer = 'mycert.server.example.com'
    userDatabaseName = 'names.nsf'
    mailFileAction = 2
}

// put your own data here
first = 'tuFirst'
last = 'tuLast'
certorg = '/ACME'

// Create Account Attribute, no need to change it
create {
    FirstName = first
    LastName = last
    __NAME__ = "${first} ${last} ${certorg}".toString()
    ShortName = first[0].toLowerCase() + last
    __PASSWORD__ = new GuardedString("somepassword1".toCharArray())
    CertifierOrgHierarchy = certorg
}

// Update Account Attribute, no need to change it
update {
    FirstName = "updated"
}

// Flag if the created account should be deleted, comment the whole section if
you don't want the user to be deleted
delete {
}

<<<<< end of example-config.groovy <<<<<<<
```

This file is divided into the following sections:



- The "ICF section, which includes the following properties

| Property Name                                  | Description  |
|--|--|
| bundleName,<br>bundleVersion,<br>connectorName | Denotes which Identity connector should be used by the test-utility. This information is preconfigured for the Domino Identity Connector, so no changes are required here. |
| connectorServer                                | Update this section based on your environment.   |
| host   | Connector Server host (hostname or IP address)   |
| port   | Connector Server port  |
| key  | Connector Server key   |

- The Connector section contains configuration information that is specific to the Identity connector and it is similar to the IT Resource configuration in OIM. The configuration properties in this section are the same as those in the Lotus Notes IT Resource.

**Table 5-1 IT Resource Parameters**

| Parameter            | Description  |
|----------------------|--|
| adminIdFile          | Fully-qualified path to the Administrator ID file.<br>For example: C:\Lotus\Notes\Data\admin.id  |
| adminName            | Administrator account name, such as Administrator/ACM  |
| adminPassword        | Administrator password.  |
| administrationServer | Name of the host where the administration server is running.   |
| certifierIdFile      | Fully-qualified path to the Certifier ID file.<br>For example: C:\Lotus\Domino\Data\cert.id  |
| certifierPassword    | Password for the specified Certifier ID file.  |
| createIdFile         | Enter True if you want a mail file to be created with the ID file when the Register New User function of IBM Lotus Notes and Domino is called. Otherwise, enter False.<br>Default is: True.  |
| createMailDB         | Indicates whether to set up mail when a user is created. If checked (True), mail setup occurs at account creation. If unchecked (False), mail setup occurs at first login.<br>Default is: True.  |
| MailFileAction       | Use this parameter to specify how mail file deletion must be performed when a user is deleted.<br>You can specify one of the following values: <ul style="list-style-type: none"> <li>– Delete None (0): Specifying this value leaves the users mail file.</li> <li>– Delete Home (1): Specifying this value deletes the mail file on the users home server.</li> <li>– Delete All (2): Specifying this value deletes the mail file on the users home server and all replicas.</li> </ul> Default is: 2. |
| registrationServer   | Enter the canonical name of the server to be used when creating IDs and performing other registration functions.<br>Sample value: CN=MyServer/OU=MyOrg   |

**Table 5-1 (Cont.) IT Resource Parameters**

| Parameter        | Description                                |
|------------------|--|
| userDatabaseName | Specify the filename of the user database. |

**5. Run the following command:**

```
java -classpath ./test-utility.jar oracle.iam.connectors.testutility.Main
example-config.groovy
```

You should see output similar to this:

```
jThread Id: 1    Time: 2011-04-19 20:22:21.316    Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest    Level: OK
Message: Using remote connection info [{host=myhost.oracle.com, port=8759}]
Thread Id: 1    Time: 2011-04-19 20:22:32.065    Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest    Level: OK
Message: Using ConnectorKey [ConnectorKey(
bundleName=org.identityconnectors.domino bundleVersion=2.0.1
connectorName=org.identityconnectors.domino.DominoConnector )]
Thread Id: 1    Time: 2011-04-19 20:22:32.065    Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest    Level: OK
Message: Using ConnectorInfo
[org.identityconnectors.framework.impl.api.remote.RemoteConnectorInfoImpl@12d26d2
]
Thread Id: 1    Time: 2011-04-19 20:22:32.067    Class:
oracle.iam.connectors.testutility.TestUtility
Method: doTest    Level: INFO    Message: Connector configured
Thread Id: 1    Time: 2011-04-19 20:22:32.081    Class:
oracle.iam.connectors.testutility.TestUtility
Method: doTest    Level: INFO    Message: Got Connector Instance, ready to do the
tests
Thread Id: 1    Time: 2011-04-19 20:22:32.086    Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest    Level: INFO
Message: Running 'test' operation on connector
Thread Id: 1    Time: 2011-04-19 20:22:32.086    Class:
org.identityconnectors.framework.api.operations.TestApiOp    Method: test
Level: OK Message: Enter: test()
Thread Id: 1    Time: 2011-04-19 20:22:39.333    Class:
org.identityconnectors.framework.api.operations.TestApiOp    Method: test
Level: OK Message: Return: null
Thread Id: 1    Time: 2011-04-19 20:22:39.333    Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest    Level: INFO
Message: 'test' operation succeeded
Thread Id: 1    Time: 2011-04-19 20:22:39.333    Class:
oracle.iam.connectors.testutility.TestUtility    Method: doTest    Level: INFO
Message: Running 'create' operation on connector
... etc
```

## 5.2 Troubleshooting

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

| Problem Description  | Solution   |
|--|--|
| nlsxbe.dll is not found.   | <ul style="list-style-type: none"> <li>• Ensure that Notes install directory is included in PATH.</li> <li>• Set LD_LIBRARY_PATH to Notes Install directory.</li> </ul> <p><b>Note:</b> It is not recommended to have Domino Server &amp; Lotus Notes on the same server. If you do so for testing purpose, ensure that the LD_LIBRARY_PATH points to Notes directory and not Domino directory. Also Domino install location should not be part of PATH variable. This may conflict proper working of connector.</p> |
| Oracle Identity Manager cannot establish a connection with the IBM Lotus Notes and Domino server.                    | <ul style="list-style-type: none"> <li>• Ensure that the IBM Lotus Notes and Domino server is running.</li> <li>• Ensure that Oracle Identity Manager is running.</li> <li>• Ensure that all the adapters have been compiled.</li> <li>• Use the IT Resources form to examine the Oracle Identity Manager record.</li> </ul>   |
| An Operation Failed message is displayed on the Oracle Identity Manager Administrative and User Console              | <ul style="list-style-type: none"> <li>• Ensure that the attribute values do not contain delimiter characters (white space).</li> <li>• Ensure that the attribute values do not exceed the specified length.</li> </ul>  |
| 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>)   | <p>The name of the mail template file specified as the value of the <b>MailTemplateName</b> 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.</p> <p>For example, the name of the mail template file for IBM Lotus Notes and Domino Server version 6.x is mail6.ntf.</p>   |
| <p>Following error encountered when user is updated:</p> <pre>java.lang.IllegalArgumentException : Invalid Uid</pre> | When you manually push the certorg data to the lookup definition, ensure that the case sensitivity of the certorg data is retained.  |

| Problem Description   | Solution  |
|---|---|
| <p>Following error is encountered when you modify the account after running the target user reconciliation:</p> <pre>error occurred in oracle.iam.provisioning.handlers.ModifyAppInstanceAccountActionHandler while modifying account with key 563 associated to user with key 9004 and the cause of the error is An error occurred in oracle.iam.provisioning.spi.DOBProvisioningMechanism/modify while modifying account with account id 563 for user ERROR and the cause of error is Thor.API.Exceptions.tcAPIException : Error occurred while setting form data for process instance with key 1271.. oracle.iam.ui.platform.exception.OIMRuntimeException: IAM-40600019 : An error occurred in oracle.iam.provisioning.handlers.ModifyAppInstanceAccountActionHandler while modifying account with key 563 associated to user with key 9004 and the cause of the error is An error occurred in oracle.iam.provisioning.spi.DOBProvisioningMechanism/modify while modifying account with account id 563 for user ERROR and the cause of error is Thor.API.Exceptions.tcAPIException : Error occurred while setting form data for process instance with key 1271.. at oracle.iam.ui.platform.exception.OIMErrorHandler.reportServiceException(OIMErrorHandler.java:178) at oracle.iam.ui.platform.exception.OIMErrorHandler.reportException(OIMErrorHandler.java:66) at oracle.adf.model.binding.DCDataControl.reportException(DCDataControl.java:429) at oracle.adf.model.binding.DCBindingContainer.reportException(DCBindingContainer.java:448) at oracle.adf.model.binding.DCBindingContainer.reportException(DCBindingContainer.java:503) at oracle.adf.model.binding.DCControlBinding.reportException(DCControlBinding.java:208) at</pre> | <p>As a workaaround, perform the following steps:</p> <ol style="list-style-type: none"><li data-bbox="651 317 1372 373">1. On the Design Console, select the <b>UD_LOTUS</b> form from the form designer</li><li data-bbox="651 394 1372 451">2. Create a new version of the form, click <b>Properties</b>, and remove the required property from <b>Password</b> field.</li><li data-bbox="651 472 1372 495">3. Save the form and activate the new version.</li></ol> |

**Problem Description****Solution**

```
oracle.jbo.uicli.binding.JUCtrlActionBinding.reportException(JUCtrlActionBinding.java:2292) at
oracle.jbo.uicli.binding.JUCtrlActionBinding.doIt(JUCtrlActionBinding.java:1848) at
oracle.adf.model.binding.DCDataControl.invokeOperation(DCDataControl.java:2350) at
oracle.jbo.uicli.binding.JUCtrlActionBinding.invoke(JUCtrlActionBinding.java:835) at
oracle.adf.controller.v2.lifecycle.PageLifecycleImpl.executeEvent(PageLifecycleImpl.java:414) at
oracle.adfinternal.view.faces.model.binding.FacesCtrlActionBinding._execute(FacesCtrlActionBinding.java:257) at
oracle.adfinternal.view.faces.model.binding.FacesCtrlActionBinding.execute(FacesCtrlActionBinding.java:215) at
oracle.iam.ui.platform.utils.FacesUtils.executeOperationBinding(FacesUtils.java:188) at
oracle.iam.ui.platform.utils.FacesUtils.executeOperationBindingFromActionListener(FacesUtils.java:130) at
oracle.iam.ui.catalog.view.backing.CartReqBean.submit(CartReqBean.java:1250) at
oracle.iam.ui.catalog.view.backing.CartReqBean.submitActionListener(CartReqBean.java:1152) at
sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at
sun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:62) at
sun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:43) at
java.lang.reflect.Method.invoke(Method.java:498) at
com.sun.el.util.ReflectionUtil.invokeMethod(ReflectionUtil.java:181) at
com.sun.el.parser.AstValue.invoke(AstValue.java:289) at
com.sun.el.MethodExpressionImpl.invoke(MethodExpressionImpl.java:304) at
org.apache.myfaces.trinidadinterna
```

---

**Problem Description****Solution**

---

```
l.taglib.util.MethodExpressionMethodBinding.invoke(MethodExpressionMethodBinding.java:62) at
org.apache.myfaces.trinidad.component.UIXComponentBase.broadcastToMethodBinding(UIXComponentBase.java:2028) at
org.apache.myfaces.trinidad.component.UIXCommand.broadcast(UIXCommand.java:183) at
org.apache.myfaces.trinidad.component.UIXComponent.broadcastInContext(UIXComponent.java:373) at
oracle.adf.view.rich.event.ProxyEvent.broadcastWrappedEvent(ProxyEvent.java:72) at
oracle.adf.view.rich.component.fragment.UIXRegion._handleProxyEvent(UIXRegion.java:939)
```

---

# 6

## Known Issues and Workarounds

This chapter describes known issues and workarounds associated with this release of the connector.

### 6.1 Lotus Resource not Shown in Self Service UI

 **Note:**

This is an issue associated with the server.

Lotus resource is not shown in self service UI for user password change.

**Workaround:**

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Form Designer**.
4. Search for and open the **UD\_LOTUS** form.
5. Click **Create New Version**.
6. Change the existing label from **UD\_LOTUS\_USERPWS** to **UD\_LOTUS\_PASSWORD**.
7. Save and close the form.
8. Activate the new form.
9. Open the **Password Updated** task from process definition.
10. Change the mappings to reflect the new label.

 **Note:**

This issue is observed in Oracle Identity Manager release 11.1.2.0.0 and any BP in this release track.