Contents

Preface ......................................................................................................................................................... ix
  Audience ................................................................................................................................................... ix
  Documentation Accessibility ...................................................................................................................... ix
  Related Documents ................................................................................................................................. ix
  Documentation Updates .......................................................................................................................... ix
  Conventions ............................................................................................................................................. x

What’s New in Oracle Identity Manager Connector for Oracle CRM On Demand?........................................ xi
  Software Updates ....................................................................................................................................... xi
  Documentation-Specific Updates .............................................................................................................. xi

1 About the Connector
  1.1 Certified Components ........................................................................................................................ 1-1
  1.2 Certified Languages ............................................................................................................................. 1-2
  1.3 Connector Architecture ....................................................................................................................... 1-3
    1.3.1 Reconciliation Process ................................................................................................................ 1-4
    1.3.2 Provisioning Process .................................................................................................................... 1-5
    1.3.3 Provisioning Functions ............................................................................................................... 1-5
  1.4 Features of the Connector .................................................................................................................. 1-6
    1.4.1 ICF Based Connector ................................................................................................................... 1-6
    1.4.2 Support for Target Resource Reconciliation ........................................................................... 1-7
    1.4.3 Support for Both Full and Incremental Reconciliation ............................................................. 1-7
    1.4.4 Support for Limited Reconciliation .......................................................................................... 1-7
    1.4.5 Support for Adding Custom Attributes for Reconciliation and Provisioning ..................... 1-7
    1.4.6 Support for Transformation of Data .......................................................................................... 1-7
    1.4.7 Support for Validation of Data .................................................................................................... 1-7
    1.4.8 Support for Resource Exclusion Lists ...................................................................................... 1-7
  1.5 User Attributes for Target Resource Reconciliation and Provisioning ............................................. 1-8
  1.6 Roadmap for Deploying and Using the Connector ............................................................................ 1-8

2 Deploying the Connector
  2.1 Preinstallation ..................................................................................................................................... 2-1
    2.1.1 Files and Directories on the Installation Media ........................................................................... 2-1
    2.1.2 Configuring the Oracle WebLogic Server to Use JSSE-based SSL ....................................... 2-2
3 Using the Connector

3.1 Configuring Reconciliation ................................................................. 3-1
3.1.1 Full Reconciliation ........................................................................ 3-2
3.1.2 Limited Reconciliation .................................................................. 3-2
3.1.3 Reconciliation Rule for Target Resource Reconciliation .............. 3-2
3.1.4 Reconciliation Action Rules for Target Resource Reconciliation .... 3-3
3.2 Scheduled Jobs .................................................................................. 3-4
3.2.1 Scheduled Job for Lookup Field Synchronization ......................... 3-4
3.2.2 Scheduled Job for Reconciliation .................................................. 3-4
3.2.3 Configuring Scheduled Jobs ......................................................... 3-5
3.3 Configuring Provisioning in Oracle Identity Manager Release 11.1.1 .................. 3-6
3.3.1 Guidelines on Performing Provisioning Operations ................. 3-7
3.3.2 Configuring Direct Provisioning ................................................... 3-7
3.3.3 Configuring Request-Based Provisioning ..................................... 3-8
3.3.3.1 End User’s Role in Request-Based Provisioning .................. 3-9
3.3.3.2 Approver’s Role in Request-Based Provisioning .................. 3-9
3.3.3.3 Importing Request Datasets Using Deployment Manager ....... 3-10
3.3.3.4 Enabling the Auto Save Form Feature ................................ 3-10
3.3.3.5 Running the PurgeCache Utility ........................................... 3-11
3.3.4 Switching Between Request-Based Provisioning and Direct Provisioning .......... 3-11
3.4 Configuring Provisioning in Oracle Identity Manager Release 11.1.2......................... 3-12

4 Extending the Functionality of the Connector

4.1 Adding Custom Attributes for Target Resource Reconciliation................................. 4-1
4.2 Adding Custom Attributes for Provisioning................................................................. 4-6
4.3 Configuring Validation of Data During Reconciliation and Provisioning...................... 4-8
4.4 Configuring Transformation of Data During User Reconciliation............................... 4-11
4.5 Configuring Resource Exclusion Lists......................................................................... 4-12

5 Known Issues

Index
List of Figures

1–1 Architecture of the Connector ................................................................................................. 1-3
2–1 Manage IT Resource Page ....................................................................................................... 2-10
2–2 Edit IT Resource Details and Parameters Page .................................................................. 2-11
2–3 Manage IT Resource Page for Connector Server IT Resource ............................................ 2-12
2–4 Edit IT Resource Details and Parameters Page for Connector Server IT Resource .......... 2-13
3–1 Reconciliation Rule for Target Resource Reconciliation .................................................... 3-3
4–1 Adding a New Version of Process Form ................................................................................. 4-3
4–2 Adding a New Reconciliation Field ...................................................................................... 4-4
4–3 Adding an Entry to Reconciliation Lookup ........................................................................... 4-5
4–4 Adding a New Version of Process Form ................................................................................. 4-7
4–5 Adding an Entry to Provisioning Lookup .............................................................................. 4-8
<table>
<thead>
<tr>
<th>Table</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1–1</td>
<td>Certified Components</td>
<td>1-2</td>
</tr>
<tr>
<td>1–2</td>
<td>Provisioning Functions</td>
<td>1-5</td>
</tr>
<tr>
<td>1–3</td>
<td>User Attributes for Target Resource Reconciliation and Provisioning</td>
<td>1-8</td>
</tr>
<tr>
<td>2–1</td>
<td>Files and Directories On the Connector Installation Media</td>
<td>2-1</td>
</tr>
<tr>
<td>2–2</td>
<td>Parameters of the CRM On Demand IT Resource for the Target System</td>
<td>2-11</td>
</tr>
<tr>
<td>2–3</td>
<td>Parameters of the CRM On Demand Connector Server IT Resource</td>
<td>2-13</td>
</tr>
<tr>
<td>2–4</td>
<td>Entries in the Lookup.Configuration.CRMOD Lookup Definition</td>
<td>2-14</td>
</tr>
<tr>
<td>2–5</td>
<td>Entries in the Lookup.CRMOD.UM.Configuration</td>
<td>2-14</td>
</tr>
<tr>
<td>2–6</td>
<td>Entries in Lookup.CRMOD.UM.ProvAttrMap</td>
<td>2-16</td>
</tr>
<tr>
<td>2–7</td>
<td>Entries in Lookup.CRMOD.UM.ReconAttrMap</td>
<td>2-16</td>
</tr>
<tr>
<td>2–8</td>
<td>Log Levels and ODL Message Type:Level Combinations</td>
<td>2-18</td>
</tr>
<tr>
<td>3–1</td>
<td>Action Rules for Target Resource Reconciliation</td>
<td>3-3</td>
</tr>
<tr>
<td>3–2</td>
<td>Attributes of the Scheduled Job for Lookup Field Synchronization</td>
<td>3-4</td>
</tr>
<tr>
<td>3–3</td>
<td>Attributes of the Scheduled Job for Reconciliation</td>
<td>3-5</td>
</tr>
</tbody>
</table>
This guide describes the connector that is used to integrate Oracle Identity Manager with Oracle CRM On Demand.

**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, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Fusion Middleware User’s Guide for Oracle Identity Manager*.

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

http://download.oracle.com/docs/cd/E14571_01/im.htm

**Documentation Updates**

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

http://download.oracle.com/docs/cd/E22999_01/index.htm
Conventions

The following text conventions are used in this document:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that displays on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
What's New in Oracle Identity Manager Connector for Oracle CRM On Demand?

This chapter provides an overview of the updates made to the software and documentation for release 11.1.1.5.0 of the Oracle CRM On Demand connector.

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

- **Software Updates**

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- **Documentation-Specific Updates**

  These include major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

### Software Updates

The following section discusses the software updates:

#### Software Updates in Release 11.1.1.5.0

The following software update has been made in release 11.1.1.5.0:

**Support for SSL certificate in Websphere Server**

This release of the connector supports the SSL certificates in Websphere Server.

See Section 2.1.3, "Configuring the IBM Websphere to Import SSL Certificates from Target System" for more information.

### Documentation-Specific Updates

The following section discusses the documentation-specific updates:

#### Documentation-Specific Updates in Release 11.1.1.5.0

The following are documentation-specific updates in revision "7" of this guide:

- The "Connector Server" row has been added to Table 1–1, "Certified Components".
- The "JDK" row of Table 1–1, "Certified Components" has been renamed to "Connector Server JDK".
The following is a documentation-specific update in revision "6" of this guide:
The "Oracle Identity Manager" row of Table 1–1, "Certified Components" has been updated.

The following is a documentation-specific update in revision "5" of this guide:
A "Note" regarding lookup queries has been added at the beginning of Chapter 4, "Extending the Functionality of the Connector."

The following is a documentation-specific update in revision "4" of this guide:
Information about limited reconciliation has been modified in Section 3.1.2, "Limited Reconciliation."

The following are documentation-specific updates in revision "3" of this guide:
- The "Oracle Identity Manager" row in Table 1–1, "Certified Components" has been modified.
- A note has been added in the "xml/CRMOD-Datasets.xml" row of Table 2–1, "Files and Directories On the Connector Installation Media".
- The following sections have been added:
  - Section 2.3.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
  - Section 2.3.10, "Localizing Field Labels in UI Forms"
  - Section 3.3, "Configuring Provisioning in Oracle Identity Manager Release 11.1.1"
  - Section 3.4, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"
- Instructions specific to Oracle Identity Manager release 11.1.2.x have been added in the following sections:
  - Section 2.2.1, "Installing the Connector in Oracle Identity Manager"
  - Section 2.3.2, "Configuring the IT Resource for the Target System"
  - Section 2.3.3, "Configuring the IT Resource for the Connector Server"
  - Section 3.2.3, "Configuring Scheduled Jobs"
Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to integrate Oracle Identity Manager with Oracle CRM On Demand. This connector enables you to use the target system as a managed (target) resource of identity data for Oracle Identity Manager.

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

This chapter contains the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6, "Roadmap for Deploying and Using the Connector"

**Note:** In this guide, the term *Oracle Identity Manager server* refers to the computer on which Oracle Identity Manager is installed.

### 1.1 Certified Components

Table 1–1 lists the certified components for this connector.
The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
1.3 Connector Architecture

This connector enables management of target system accounts through Oracle Identity Manager. Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector

The Oracle Identity Manager Connector for Oracle CRM On Demand is an Identity Connector Framework (ICF)-based connector. ICF is a component that provides basic provisioning, reconciliation, and other functions that the connector requires.

The operations on the target system would be performed via web services exposed by Oracle CRM On Demand. The connector consumes the following CRM On Demand web services:

- **User web service**
  This web service is used for user-specific provisioning and reconciliation operations.

- **Role Management web service**
  This web service is used by the CRM On Demand Role Lookup Recon scheduled job to synchronize the roles available on the target system into the Lookup.CRMOD.Roles lookup definition.

- **Password web service**
  This web service is used for setting or changing the password of a user from Oracle Identity Manager.

The Web Service Description Language (WSDL) files and the generated web service stubs (artifacts) are packaged with the connector bundle. The connector communicates with the target system using these prepackaged stubs for all connector operations.

The connector leverages Oracle Web Service Manager (OWSM) for security-related aspects during communication with the target system. Communication between Oracle Identity Manager and Oracle CRM On Demand is encrypted with Secure Sockets Layer (SSL) for security (URL of the target system is always HTTPS).
addition, the connector uses username/token policy for message-level security during communication with the Oracle CRM On Demand web services.

The target system does not allow deletion of created user accounts. Therefore, as part of Revoke Resource operation of Oracle Identity Manager, the following changes will be made:

- On the target system, the corresponding user account is set to Inactive.
- In Oracle Identity Manager, the tasks for the corresponding user account are cancelled and the account status is set to Disabled.

The following topics describe the connector operations:

- Section 1.3.1, "Reconciliation Process"
- Section 1.3.2, "Provisioning Process"
- Section 1.3.3, "Provisioning Functions"

1.3.1 Reconciliation Process

This connector can be configured to perform target resource reconciliation. The connector enables you to create and manage target accounts for OIM Users through provisioning. In addition, data related to newly created and modified target system accounts can be reconciled and linked with existing OIM Users and provisioned resources.

See Also: Oracle Fusion Middleware Users’s Guide for Oracle Identity Manager for conceptual information about target resource reconciliation

The following is an overview of the steps involved in reconciliation:

1. The scheduled job is run at the time or frequency that you specify. This scheduled task contains details of the reconciliation that you want to perform.

2. The scheduled job performs the following tasks:
   - Reads the values that you set for the job attributes.
   - Fetches user records into Oracle Identity Manager.

3. Each user record fetched from the target system is compared with existing target system resources assigned to OIM Users. The reconciliation rule is applied during the comparison process. See Section 3.1.3, "Reconciliation Rule for Target Resource Reconciliation" for information about the reconciliation rule.

4. The next step of the process depends on the outcome of the matching operation:
   - If a match is found between the target system record and a resource provisioned to an OIM User, then the user resource is updated with changes made to the target system record.
   - If no match is found, then the target system user record is compared with existing OIM Users. The next step depends on the outcome of the matching operation:
     - If a match is found, then the target system record is used to provision a resource for the OIM User.
     - If no match is found, then the status of the reconciliation event is set to No Match Found.
1.3.2 Provisioning Process

Provisioning involves creating and managing user accounts. When you allocate (or provision) an Oracle CRM On Demand resource to an OIM User, the operation results in the creation of an account on the target system for that user. Similarly, when you update the resource on Oracle Identity Manager, the same update is made to the account on the target system.

Provisioning is a two-step process. In the first step, the create user task is triggered. If the create user task is completed successfully, then the second step is initiated. In the second step, the password update task is triggered.

During provisioning operations, adapters carry provisioning data submitted through the process form to the connector, which in turn submits the provisioning data to the target system. The user account maintenance commands accept provisioning data from the adapters, carry out the required operation on the target system, and return the response from the target system to the adapters. The adapters return the response to Oracle Identity Manager.

The provisioning process can be started through one of the following events:

- Direct provisioning
  The Oracle Identity Manager administrator uses the Administrative and User Console to create a target system account for a user.

- Provisioning triggered by access policy changes
  An access policy related to accounts on the target system is modified. When an access policy is modified, it is reevaluated for all users to which it applies.

- Request-based provisioning
  In request-based provisioning, an individual creates a request for a target system account. The provisioning process is completed when an OIM User with the required privileges approves the request and provisions the target system account to the requester.

1.3.3 Provisioning Functions

Table 1–2 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

<table>
<thead>
<tr>
<th>Function</th>
<th>Adapter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create User</td>
<td>CRMODCreateUser</td>
</tr>
<tr>
<td>Delete User</td>
<td>CRMODDisableUser</td>
</tr>
<tr>
<td>Disable User</td>
<td>CRMODDisableUser</td>
</tr>
<tr>
<td>Enable User</td>
<td>CRMODEnableUser</td>
</tr>
<tr>
<td>Alias Updated</td>
<td>CRMODUpdateUser</td>
</tr>
<tr>
<td>Cell Phone Updated</td>
<td>CRMODUpdateUser</td>
</tr>
<tr>
<td>Department Updated</td>
<td>CRMODUpdateUser</td>
</tr>
</tbody>
</table>
1.4 Features of the Connector

- Section 1.4.1, "ICF Based Connector"
- Section 1.4.2, "Support for Target Resource Reconciliation"
- Section 1.4.3, "Support for Both Full and Incremental Reconciliation"
- Section 1.4.4, "Support for Limited Reconciliation"
- Section 1.4.5, "Support for Adding Custom Attributes for Reconciliation and Provisioning"
- Section 1.4.6, "Support for Transformation of Data"
- Section 1.4.7, "Support for Validation of Data"
- Section 1.4.8, "Support for Resource Exclusion Lists"

1.4.1 ICF Based Connector

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager connectors require.

The Oracle Identity Manager Connector for Oracle CRM On Demand is an ICF-based connector. The ICF uses classpath isolation, which allows the connector to co-exist with legacy versions of the connector.

For more information about the ICF and its advantages, see the "Understanding the Identity Connector Framework" chapter in the Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager.
1.4.2 Support for Target Resource Reconciliation

You can use the connector to configure the target system as a target resource of Oracle Identity Manager.

See Section 3.1, "Configuring Reconciliation" for more information.

1.4.3 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, incremental reconciliation is automatically enabled from the next run of the user reconciliation.

You can perform a full reconciliation run at any time. See Section 3.1.1, "Full Reconciliation" for more information.

1.4.4 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of the scheduled jobs. This filter specifies the subset of newly added and modified target system records that must be reconciled.

See Section 3.1.2, "Limited Reconciliation" for more information.

1.4.5 Support for Adding Custom Attributes for Reconciliation and Provisioning

If you want to add custom attributes for reconciliation and provisioning, then perform the procedures described in Section 4.1, "Adding Custom Attributes for Target Resource Reconciliation" and Section 4.2, "Adding Custom Attributes for Provisioning."

1.4.6 Support for Transformation of Data

You can configure transformation of data that is brought into Oracle Identity Manager during reconciliation.

See Section 4.4, "Configuring Transformation of Data During User Reconciliation" for more information.

1.4.7 Support for Validation of Data

You can configure validation of data that is brought into Oracle Identity Manager during provisioning and reconciliation operations.

See Section 4.3, "Configuring Validation of Data During Reconciliation and Provisioning" for more information.

1.4.8 Support for Resource Exclusion Lists

You can specify a list of accounts that must be excluded from reconciliation and provisioning operations. Accounts whose user IDs you specify in the exclusion list are not affected by reconciliation and provisioning operations.

Section 4.5, "Configuring Resource Exclusion Lists" describes the procedure to add entries in these lookup definitions.
1.5 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 provides information about user attribute mappings for target resource reconciliation and provisioning.

<table>
<thead>
<tr>
<th>Process Form Field</th>
<th>Target System Field (User Schema)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Alias</td>
<td>Alias of the user</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>CellPhone</td>
<td>Cell phone number of the user</td>
</tr>
<tr>
<td>Department</td>
<td>Department</td>
<td>Department of the user</td>
</tr>
<tr>
<td>Division</td>
<td>Division</td>
<td>Division of the user</td>
</tr>
<tr>
<td>Email</td>
<td>EmailAddr</td>
<td>Email ID of the user</td>
</tr>
<tr>
<td>Employee Number</td>
<td>EmployeeNumber</td>
<td>Employee number of the user</td>
</tr>
<tr>
<td>First Name</td>
<td>FirstName</td>
<td>First name of the user</td>
</tr>
<tr>
<td>Job Title</td>
<td>JobTitle</td>
<td>Job title of the user</td>
</tr>
<tr>
<td>Last Name</td>
<td>LastName</td>
<td>Last name of the user</td>
</tr>
<tr>
<td>Middle Name</td>
<td>MiddleName</td>
<td>Middle name of the user</td>
</tr>
<tr>
<td>Password</td>
<td><strong>PASSWORD</strong></td>
<td>User’s password</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Note:</strong> The Password field can only be updated. It cannot be reconciled.</td>
</tr>
<tr>
<td>Region</td>
<td>Region</td>
<td>Region of the user</td>
</tr>
<tr>
<td>Return ID</td>
<td><strong>UID</strong></td>
<td>UID of the user</td>
</tr>
<tr>
<td>Role[LOOKUP]</td>
<td>Role</td>
<td>User’s role</td>
</tr>
<tr>
<td>User Login Id</td>
<td>UserLoginId</td>
<td>User’s login ID</td>
</tr>
<tr>
<td>Work Phone</td>
<td>PhoneNumber</td>
<td>Phone number of the user</td>
</tr>
</tbody>
</table>

1.6 Roadmap for Deploying and Using the Connector

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

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

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"
- Section 2.4, "Postcloning Steps"

2.1 Preinstallation

Preinstallation information is available in the following section:

- Section 2.1.1, "Files and Directories on the Installation Media"
- Section 2.1.2, "Configuring the Oracle WebLogic Server to Use JSSE-based SSL"
- Section 2.1.3, "Configuring the IBM Websphere to Import SSL Certificates from Target System"

2.1.1 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 2–1.

<table>
<thead>
<tr>
<th>File in the Installation Media Directory</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bundle/org.identityconnectors.cmod-1.0.0001</td>
<td>This JAR file contains the connector bundle.</td>
</tr>
<tr>
<td>configuration/CROMD-CI.xml</td>
<td>This XML file contains configuration information that is used during the connector installation process.</td>
</tr>
</tbody>
</table>
2.1.2 Configuring the Oracle WebLogic Server to Use JSSE-based SSL

Java Secure Socket Extension (JSSE) is the Java standard framework for SSL and TLS and includes both blocking-IO and non-blocking-IO APIs, and a reference implementation including several commonly-trusted CAs.

To enable the JSSE-based SSL implementation in WebLogic Server:

1. Log in to Oracle WebLogic Administration Console.
2. Expand Environment, Servers.
3. Click on the server on which Oracle Identity Manager is deployed.
   For example: oim_server
4. On the SSL tab, click Advanced.
5. Select the Use JSSE SSL check box.

Note: Perform the procedure described in this section only if you are deploying the connector bundle on the computer hosting Oracle Identity Manager.

You can skip this section if you are deploying the connector bundle on the Connector Server.

Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.

Note: Use this file only if you are using Oracle Identity Manager release prior to 11.1.2.
If the check box is not enabled, then click **Lock and Edit** in the left pane.

6. Click the save icon.

7. If you are deploying the connector in a clustered environment, then repeat the steps from Step 3 to Step 6 for each node in the cluster.

8. Restart Oracle Identity Manager and Admin Server.

### 2.1.3 Configuring the IBM Websphere to Import SSL Certificates from Target System

**Note:** Perform the procedure described in this section only if you are deploying the connector bundle on the computer hosting Oracle Identity Manager. This section can be skipped, if you are deploying the connector bundle on the Connector Server.

To enable the SSL certificate in Websphere Server:

1. Log into the administrative console.

2. Expand Security and click **SSL certificate** and **key management.** Under Configuration settings, click **Manage endpoint security configurations.**

3. Select the appropriate outbound configuration to get to the (cell):DefaultCell01 management scope.

4. Under Related Items, click **Key stores** and certificates and click the **CellDefaultTrustStore key store.**

5. Under Additional Properties, click **Signer certificates and Retrieve** from Port.

6. In the Host field, enter the host name field, Port field and Alias field.
   - **For example:**
     - Host Name: `secure-ausomxdsa.crmondemand.com`
     - Port: `443`
     - Alias: `secure-ausomxdsa.crmondemand.com_cert`

7. Click Retrieve Signer Information.

8. Verify that the certificate information is for a certificate that you can trust.

9. Click **Apply** and Save.

10. Restart the Oracle Identity Manager and Admin Server.

### 2.2 Installation

Depending on where you want to run the connector code (bundle), the connector provides the following installation options:

- To run the connector code locally in Oracle Identity Manager, perform the procedure described in Section 2.2.1, "Installing the Connector in Oracle Identity Manager."

- To run the connector code remotely in a Connector Server, perform the procedures described in Section 2.2.1, "Installing the Connector in Oracle Identity Manager" and Section 2.2.2, "Deploying the Connector Bundle in a Connector Server."
2.2.1 Installing the Connector in Oracle Identity Manager

In this scenario, you install the connector in Oracle Identity Manager using the Connector Installer.

---

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

---

To run the Connector Installer:

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

   \( OIM\_HOME/\text{server/ConnectorDefaultDirectory} \)

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

   - For Oracle Identity Manager release 11.1.1:
     a. Log in to the Administrative and User Console by using the user account described in the “Creating the User Account for Installing Connectors” section *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager*.
     b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click *Manage Connector*.

   - For Oracle Identity Manager release 11.1.2.x:
     a. Log in to Oracle Identity System Administration by using the user account described in the “Creating the User Account for Installing Connectors” section *Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager*.
     b. In the left pane, under System Management, click *Manage Connector*.

3. In the Manage Connector page, click *Install*.

4. From the Connector List list, select *Oracle CRM On Demand Connector 11.1.1.5.0*. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation 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 *Oracle CRM On Demand Connector 11.1.1.5.0*.

5. Click *Load*.

6. To start the installation process, click *Continue*.

   The following tasks are performed, in sequence:

   a. Configuration of connector libraries
   b. Import of the connector XML files (by using the Deployment Manager)
   c. Compilation of adapters
On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

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

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

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

---

**Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.9, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.

There are no prerequisites for some predefined connectors.

---

b. Configuring the IT resource for the connector

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

c. Configuring the scheduled jobs

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.

### 2.2.2 Deploying the Connector Bundle in a Connector Server

To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in Section 2.2.1, "Installing the Connector in Oracle Identity Manager."

---

**Note:**

- You can download the Connector Server from the Oracle Technology Network web page.
- See Section 2.3.3, "Configuring the IT Resource for the Connector Server" for related information.
- See "Using an Identity Connector Server" section in the Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for more information about installing, configuring, and running the Connector Server.

---

To install the connector in the Connector Server:
1. Stop the Connector Server.

2. Copy the connector bundle JAR file from the bundle directory of the connector installation media into the following directory:

   CONNECTOR_SERVER_HOME/bundles

3. Copy the following file on the computer running Oracle Identity Manager to the CONNECTOR_SERVER_HOME/lib directory:

   ORACLE_COMMON/modules/oracle.webservices_11.1.1/oracle.webservices.standalone.client.jar

---

**Note:** If the Oracle Identity Manager is deployed on Websphere, then copy the additional jars as mentioned below to CONNECTOR_SERVER_HOME/lib:

1. ORACLE_COMMON/webservices/wsclient_extended.jar
2. ORACLE_COMMON/modules/oracle.adf.share.ca_11.1.1/ADF-SHARE-CA.jar

4. Copy the following file on the computer running Oracle Identity Manager to the CONNECTOR_SERVER_HOME/conf directory:

   For Weblogic:
   
   $DOMAIN_HOME/config/fmwconfig/jps-config-jse.xml

   For Websphere:
   
   $PROFILE_HOME/config/cells/DefaultCell01/fmwconfig/jps-config-jse.xml

5. From the CONNECTOR_SERVER_HOME/bin directory, open the ConnectorServer.bat file. Then, replace the line that starts with set JAVA_OPTS with the following line:

   `set JAVA_OPTS=-Xmx500m
   -Djava.util.logging.config.file=%CONNECTOR_SERVER_HOME%\conf\logging.properties
   -Djava.io.tmpdir=%CONNECTOR_SERVER_HOME%\temp
   -Doracle.security.jps.config=%CONNECTOR_SERVER_HOME%\conf\jps-config-jse.xml`


### 2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Section 2.3.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
- Section 2.3.2, "Configuring the IT Resource for the Target System"
- Section 2.3.3, "Configuring the IT Resource for the Connector Server"
- Section 2.3.4, "Setting up the Lookup Definition for Connector Configuration"
- Section 2.3.5, "Setting up the Lookup Definition for User Operations"
- Section 2.3.6, "Setting up the Lookup Definitions for Attribute Mappings"
- Section 2.3.7, "Enabling Logging"
- Section 2.3.8, "Changing to the Required Input Locale"
- Section 2.3.9, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.10, "Localizing Field Labels in UI Forms"
2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

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

- Section 2.3.1.1, "Creating and Activating a Sandbox"
- Section 2.3.1.2, "Creating a New UI Form"
- Section 2.3.1.3, "Creating an Application Instance"
- Section 2.3.1.4, "Publishing a Sandbox"
- Section 2.3.1.5, "Syncing Catalog"
- Section 2.3.1.6, "Updating an Existing Application Instance with a New Form"
- Section 2.3.1.7, "Configuring Form Fields"

2.3.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see the "Managing Sandboxes" section in the Oracle Fusion Middleware Administrator’s Guide 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.

The sandbox is activated.

2.3.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see the "Managing Forms" chapter in the Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager.

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, such as CRM On Demand.
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 the "Managing Application Instances" chapter in the Oracle Fusion Middleware Administrator’s Guide for 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.
   For example, select Resource Object as CRM On Demand and IT Resource Instance of type CRM On Demand in the Search box.
4. In the Form drop-down list, select the newly created form and click Apply.
5. Publish the application instance for a particular organization.

2.3.1.4 Publishing a Sandbox
To publish the sandbox that you created in Section 2.3.1.1, "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 Section 2.3.1.1, "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 Syncing Catalog
To sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Section 3.2.1, "Scheduled Job for Lookup Field Synchronization."
2. Run the Catalog Synchronization Job scheduled job. See the "Predefined Scheduled Tasks" section in the Oracle Fusion Middleware Administrator’s Guide for 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 Section 2.3.1.1, "Creating and Activating a Sandbox."
2. Create a new UI form for the resource as described in Section 2.3.1.2, "Creating a New UI Form."
3. Open the existing application instance.
4. In the Form field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in Section 2.3.1.4, "Publishing a Sandbox."

2.3.1.7 Configuring Form Fields
After installing the connector, you must configure some fields on the parent form in Oracle Identity Manager release 11.1.2.x or later. To do so:

1. Log in to Oracle Identity System Administration.
2. In the left pane, under Configuration, click Form Designer.
3. Enter UD_CRMOD_U 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. Click the Properties tab.
8. To display Account Name in the Accounts tab of the user, select the User Login Id field, and click Add Property.
9. From the Property Name list, select AccountName.
10. In the Property Value field, enter true.
11. To represent the immutable GUID of the specific account used for Oracle Identity Analytics (OIA) integration, select the Return Id field, and click Add Property.
12. From the Property Name list, select AccountId.
13. In the Property Value field, enter true.
14. To identify the ITResource field, select the CRMOD IT Resource field, and click Add Property.
15. From the Property Name list, select ITResource.
16. In the Property Value field, enter true.
17. Click Save.
18. Click Make Version Active.
19. Update the application instance with the new form as described in Section 2.3.1.6, "Updating an Existing Application Instance with a New Form."

2.3.2 Configuring the IT Resource for the Target System
The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information for reconciliation and provisioning.

For both provisioning and reconciliation, the connector uses the CRM On Demand IT Resource. This IT resource is created with default parameter values as part of the connector installation. You must update the IT resource parameters with information about the target system.

To configure the CRM On Demand IT resource:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   ■ For Oracle Identity Manager release 11.1.1:
Log in to the Administrative and User Console

- For Oracle Identity Manager release 11.1.2.x:
  Log in to Oracle Identity System Administration

2. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click Advanced in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click Manage IT Resource.

3. If you are using Oracle Identity Manager release 11.1.2.x, then in the left pane under Configuration, click IT Resource.

4. In the IT Resource Name field on the Manage IT Resource page, enter CRM On Demand and then click Search. Figure 2–1 shows the Manage IT Resource page.

**Figure 2–1 Manage IT Resource Page**

![Manage IT Resource Page](image)

5. Click the edit icon corresponding to the CRM On Demand IT resource.

6. From the list at the top of the page, select Details and Parameters.

7. Specify values for the parameters of the CRM On Demand IT resource. Figure 2–2 shows the Edit IT Resource Details and Parameters page.
Figure 2–2  Edit IT Resource Details and Parameters Page

Table 2–2 describes each parameter of the CRM On Demand IT resource.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Lookup</td>
<td>Name of the lookup definition that stores configuration information used during reconciliation and provisioning</td>
</tr>
<tr>
<td></td>
<td>Default value: Lookup.Configuration.CRMOD</td>
</tr>
<tr>
<td>Connector Server Name</td>
<td>Name of the IT resource of type &quot;Connector Server&quot;</td>
</tr>
<tr>
<td></td>
<td>By default, this field is blank.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> There is no separate IT resource created for the Connector Server during the connector installation. If you are using a Connector Server, then you must create a separate IT resource and specify its name in this field. See Section 2.3.3, “Configuring the IT Resource for the Connector Server” for information about modifying the IT resource attributes.</td>
</tr>
<tr>
<td>adminID</td>
<td>User ID of the administrator to perform connector operations</td>
</tr>
<tr>
<td></td>
<td>Sample value: GPIANOSI13-19/JOHN.DOE</td>
</tr>
<tr>
<td>adminPassword</td>
<td>Password of the administrator</td>
</tr>
<tr>
<td>targetUrl</td>
<td>URL of the Oracle CRM On Demand target system. Note: The value of this field must not contain '/' (forward slash character) at the end.</td>
</tr>
</tbody>
</table>

8. To save the values, click Update.

2.3.3 Configuring the IT Resource for the Connector Server

Perform the procedure described in this section only if you have installed the connector bundle in a Connector Server, as described in Section 2.2.2, "Deploying the Connector Bundle in a Connector Server." You must create a separate IT resource for the Connector Server.

To configure or modify the IT resource for the Connector Server:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
For Oracle Identity Manager release 11.1.1:
Log in to the Administrative and User Console

For Oracle Identity Manager release 11.1.2.x:
Log in to Oracle Identity System Administration

2. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.

3. If you are using Oracle Identity Manager release 11.1.2.x, then in the left pane under Configuration, click **IT Resource**.

4. In the IT Resource Name field on the Manage IT Resource page, enter the name of the IT resource for the Connector Server. For example, **Local**. Then, click **Search**. **Figure 2–3** shows the Manage IT Resource page.

   **Figure 2–3  Manage IT Resource Page for Connector Server IT Resource**

5. Click the edit icon corresponding to the Connector Server IT resource.

6. From the list at the top of the page, select **Details and Parameters**.

7. Specify values for the parameters of the Connector Server IT resource. **Figure 2–4** shows the Edit IT Resource Details and Parameters page.
Table 2–3 provides information about the parameters of the IT resource.

**Table 2–3 Parameters of the CRM On Demand Connector Server IT Resource**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Enter the host name or IP address of the computer hosting the Connector Server. Sample value: HostName</td>
</tr>
<tr>
<td>Key</td>
<td>Enter the key for the Connector Server.</td>
</tr>
<tr>
<td>Port</td>
<td>Enter the number of the port at which the Connector Server is listening. By default, this value is blank. You must enter the port number that is displayed on the terminal when you start the Connector Server. For example: 8759</td>
</tr>
<tr>
<td>Timeout</td>
<td>Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Manager times out. If the value is zero or if no value is specified, the connection will not timeout. Recommended value: 0</td>
</tr>
<tr>
<td>UseSSL</td>
<td>Enter <em>yes</em> to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter <em>no</em>. Default value: <em>no</em></td>
</tr>
</tbody>
</table>

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

**2.3.4 Setting up the Lookup Definition for Connector Configuration**

The Lookup.Configuration.CRMOD lookup definition is created in Oracle Identity Manager when you deploy the connector. This lookup definition holds connector configuration entries that are used during reconciliation and provisioning operations. *Table 2–4* lists the default entries in these lookup definitions.
Table 2-4  Entries in the Lookup.Configuration.CMOD Lookup Definition

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle Name</td>
<td>org.identityconnectors.crmod</td>
<td>Name of the connector bundle package</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not modify this entry.</td>
</tr>
<tr>
<td>Bundle Version</td>
<td>1.0.0001</td>
<td>Version of the connector bundle class</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not modify this entry.</td>
</tr>
<tr>
<td>Connector Name</td>
<td>org.identityconnectors.crmod.CMODConnector</td>
<td>Name of the connector class</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not modify this entry.</td>
</tr>
<tr>
<td>User Configuration Lookup</td>
<td>Lookup.CROMOD.UM.Configuration</td>
<td>Name of the lookup definition that contains user-specific configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do not modify this entry.</td>
</tr>
</tbody>
</table>

2.3.5 Setting up the Lookup Definition for User Operations

The Lookup.CROMOD.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations.

Table 2-5 lists the default entries in this lookup definition.

Table 2–5  Entries in the Lookup.CROMOD.UM.Configuration

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Attribute Map</td>
<td>Lookup.CROMOD.UM.ProvAttrMap</td>
<td>This entry holds the name of the lookup definition that maps process form</td>
</tr>
<tr>
<td></td>
<td></td>
<td>fields and attributes in User Generic WSDL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 2.3.6.1, &quot;Lookup.CROMOD.UM.ProvAttrMap&quot; for more information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>about this lookup definition.</td>
</tr>
<tr>
<td>Recon Attribute Map</td>
<td>Lookup.CROMOD.UM.ReconAttrMap</td>
<td>This entry holds the name of the lookup definition that maps resource</td>
</tr>
<tr>
<td></td>
<td></td>
<td>object fields and attributes in User Generic WSDL.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 2.3.6.2, &quot;Lookup.CROMOD.UM.ReconAttrMap&quot; for more information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>about this lookup definition.</td>
</tr>
<tr>
<td>Recon Transformation Lookup</td>
<td>Lookup.CROMOD.UM.ReconTransformations</td>
<td>This entry holds the name of the lookup definition that is used to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>configure transformation of attribute values that are fetched from the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>target system during user reconciliation.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See Section 4.4, &quot;Configuring Transformation of Data During User</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reconciliation&quot; for more information about adding entries in this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>lookup definition.</td>
</tr>
</tbody>
</table>
2.3.6 Setting up the Lookup Definitions for Attribute Mappings

The attribute mapping lookup definitions are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed. The lookup definitions are as follows:

- **Section 2.3.6.1**, "Lookup.CRMOD.UM.ProvAttrMap"
- **Section 2.3.6.2**, "Lookup.CRMOD.UM.ReconAttrMap"
- **Section 2.3.6.3**, "Lookup.CRMOD.Roles"
- **Section 2.3.6.4**, "Lookup.CRMOD.Languages"

### Table 2–5 (Cont.) Entries in the Lookup.CRMOD.UM.Configuration

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provisioning Validation Lookup</td>
<td>Lookup.CRMOD.UM.ProvValidations</td>
<td>This entry holds the name of the lookup definition that is used to configure validation of attribute values entered on the process form during provisioning operations. See Section 4.3, &quot;Configuring Validation of Data During Reconciliation and Provisioning&quot; for more information about adding entries in this lookup definition.</td>
</tr>
<tr>
<td>Recon Validation Lookup</td>
<td>Lookup.CRMOD.UM.ReconValidation</td>
<td>This entry holds the name of the lookup definition that is used to configure validation of attribute values that are fetched from the target system during reconciliation. See Section 4.3, &quot;Configuring Validation of Data During Reconciliation and Provisioning&quot; for more information about adding entries in this lookup definition.</td>
</tr>
<tr>
<td>Provisioning Exclusion Lookup</td>
<td>Lookup.CRMOD.UM.ProvExclusionList</td>
<td>This entry holds the name of the lookup definition that is used to configure resource exclusion lists during reconciliation. See Section 4.5, &quot;Configuring Resource Exclusion Lists&quot; for more information.</td>
</tr>
<tr>
<td>Recon Exclusion Lookup</td>
<td>Lookup.CRMOD.UM.ReconExclusionList</td>
<td>This entry holds the name of the lookup definition that is used to configure resource exclusion lists during provisioning operations. See Section 4.5, &quot;Configuring Resource Exclusion Lists&quot; for more information about adding entries in this lookup definition.</td>
</tr>
</tbody>
</table>

2.3.6.1 Lookup.CRMOD.UM.ProvAttrMap

The Lookup.CRMOD.UM.ProvAttrMap lookup definition holds mappings between process form fields (Code Key values) and attributes in User Generic WSDL (Decode values) used during provisioning operations.

You can add entries to this lookup if you want to map new attributes in User Generic WSDL for provisioning. See Section 4.2, "Adding Custom Attributes for Provisioning" for more information.

Table 2–6 lists the default entries in this lookup definition.
The Lookup.CRM.OD.UM.ReconAttrMap lookup definition holds mappings between resource object fields (Code Key values) and attributes in User Generic WSDL (Decode values) used during reconciliation operations.

You can add entries to this lookup definition if you want to map new attributes in User Generic WSDL for reconciliation. See Section 4.1, "Adding Custom Attributes for Target Resource Reconciliation" for more information.

Table 2-7 lists the default entries in this lookup definition.

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Alias</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>CellPhone</td>
</tr>
<tr>
<td>Department</td>
<td>Department</td>
</tr>
<tr>
<td>Division</td>
<td>Division</td>
</tr>
<tr>
<td>Email</td>
<td>EmailAddr</td>
</tr>
<tr>
<td>Employee Number</td>
<td>EmployeeNumber</td>
</tr>
<tr>
<td>External Unique ID</td>
<td>ExternalSystemId</td>
</tr>
<tr>
<td>FirstName</td>
<td>FirstName</td>
</tr>
<tr>
<td>Job Title</td>
<td>JobTitle</td>
</tr>
<tr>
<td>Language</td>
<td>Language</td>
</tr>
<tr>
<td>Last Name</td>
<td>LastName</td>
</tr>
<tr>
<td>Middle Name</td>
<td>MiddleName</td>
</tr>
<tr>
<td>Password</td>
<td><strong>PASSWORD</strong></td>
</tr>
<tr>
<td>Region</td>
<td>Region</td>
</tr>
<tr>
<td>Reports To</td>
<td>ManagerFullName</td>
</tr>
<tr>
<td>Return ID</td>
<td><strong>UID</strong></td>
</tr>
<tr>
<td>Role[LOOKUP]</td>
<td>Role</td>
</tr>
<tr>
<td>User Login Id</td>
<td>UserLoginId</td>
</tr>
<tr>
<td>Work Phone</td>
<td>PhoneNumber</td>
</tr>
</tbody>
</table>

### 2.3.6.2 Lookup.CRM.OD.UM.ReconAttrMap

The Lookup.CRM.OD.UM.ReconAttrMap lookup definition holds mappings between resource object fields (Code Key values) and attributes in User Generic WSDL (Decode values) used during reconciliation operations.

You can add entries to this lookup definition if you want to map new attributes in User Generic WSDL for reconciliation. See Section 4.1, "Adding Custom Attributes for Target Resource Reconciliation" for more information.

Table 2-7 lists the default entries in this lookup definition.

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alias</td>
<td>Alias</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>CellPhone</td>
</tr>
<tr>
<td>Department</td>
<td>Department</td>
</tr>
<tr>
<td>Division</td>
<td>Division</td>
</tr>
<tr>
<td>Email</td>
<td>EmailAddr</td>
</tr>
<tr>
<td>Employee Number</td>
<td>EmployeeNumber</td>
</tr>
<tr>
<td>External Unique ID</td>
<td>ExternalSystemId</td>
</tr>
<tr>
<td>FirstName</td>
<td>FirstName</td>
</tr>
</tbody>
</table>
2.3.6.3 Lookup.CRMOD.Roles
The Lookup.CRMOD.Roles lookup definition is used to store user roles after running the scheduled job for reconciling roles. By default, this lookup definition is empty after the connector is deployed.

2.3.6.4 Lookup.CRMOD.Languages
The Lookup.CRMOD.Languages lookup definition contains user languages. Do not modify the entries in this lookup definition.

This lookup contains the following entries by default:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinese (Simplified)</td>
<td>Chinese (Simplified)</td>
</tr>
<tr>
<td>English-American</td>
<td>English-American</td>
</tr>
<tr>
<td>English-British</td>
<td>English-British</td>
</tr>
<tr>
<td>French</td>
<td>French</td>
</tr>
<tr>
<td>German</td>
<td>German</td>
</tr>
<tr>
<td>Italian</td>
<td>Italian</td>
</tr>
<tr>
<td>Japanese</td>
<td>Japanese</td>
</tr>
<tr>
<td>Korean</td>
<td>Korean</td>
</tr>
<tr>
<td>Portuguese</td>
<td>Portuguese</td>
</tr>
<tr>
<td>Spanish</td>
<td>Spanish</td>
</tr>
</tbody>
</table>

2.3.7 Enabling Logging
Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:
In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

- SEVERE.intValue()+100
  This level enables logging of information about fatal errors.
- SEVERE
  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.
- WARNING
  This level enables logging of information about potentially harmful situations.
- INFO
  This level enables logging of messages that highlight the progress of the application.
- CONFIG
  This level enables logging of information about fine-grained events that are useful for debugging.
- FINE, FINER, FINEST
  These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in Table 2–8.

<table>
<thead>
<tr>
<th>Log Level</th>
<th>ODL Message Type:Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEVERE.intValue()+100</td>
<td>INCIDENT_ERROR:1</td>
</tr>
<tr>
<td>SEVERE</td>
<td>ERROR:1</td>
</tr>
<tr>
<td>WARNING</td>
<td>WARNING:1</td>
</tr>
<tr>
<td>INFO</td>
<td>NOTIFICATION:1</td>
</tr>
<tr>
<td>CONFIG</td>
<td>NOTIFICATION:16</td>
</tr>
<tr>
<td>FINE</td>
<td>TRACE:1</td>
</tr>
<tr>
<td>FINER</td>
<td>TRACE:16</td>
</tr>
<tr>
<td>FINEST</td>
<td>TRACE:32</td>
</tr>
</tbody>
</table>

The configuration file for OJDL is logging.xml, which is located at the following path:

```
DOMAIN_HOME/config/fmwconfig/servers/OIM_SERVER/logging.xml
```

Here, `DOMAIN_HOME` and `OIM_SERVER` are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:
   a. Add the following blocks in the file:
      ```
      <log_handler name='crmod-handler' level='[LOG_LEVEL]' />
      ```
Deploying the Connector

2-19

b. Replace both occurrences of \[LOG\_LEVEL\] with the ODL message type and level combination that you require. Table 2–8 lists the supported message type and level combinations.

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

The following blocks show sample values for \[LOG\_LEVEL\] and \[FILE\_NAME\] :

```
<log_handler name='crmod-handler' level='NOTIFICATION:1'
    class='oracle.core.ojdl.logging.ODLHandlerFactory'>
    <property name='logreader:' value='off'/>
    <property name='path' value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\oim_server1\logs\oim_server1-diagnostic-1.log'/>
    <property name='format' value='ODL-Text'/>
    <property name='useThreadName' value='true'/>
    <property name='locale' value='en'/>
    <property name='maxFileSize' value='5242880'/>
    <property name='maxLogSize' value='52428800'/>
    <property name='encoding' value='UTF-8'/>
</log_handler>

<logger name="ORG.IDENTITYCONNECTORS.CRMOD" level="[LOG_LEVEL]"
    useParentHandlers="false">
    <handler name="crmod-handler"/>
    <handler name="console-handler"/>
</logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

   For Microsoft Windows:
   ```
   set WLS_REDIRECT_LOG=FILENAME
   ```

   For UNIX:
   ```
   export WLS_REDIRECT_LOG=FILENAME
   ```
Replace FILENAME with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.3.8 Changing to the Required Input Locale

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

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.

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the 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.
2. Enter one of the following commands:

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

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

   PurgeCache.bat MetaData
   PurgeCache.sh MetaData

   **On Microsoft Windows:** PurgeCache.bat All
   **On UNIX:** PurgeCache.sh All

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

   t3://OIM_HOST_NAME:OIM_PORT_NUMBER

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

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

### 2.3.10 Localizing Field Labels in UI Forms

**Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.x or later and you want to localize UI form field labels.

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select `oracle.iam.console.identity.sysadmin.ear`.
3. In the right pane, from the Application Deployment list, select **MDS Configuration**.
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor: `SAVED_LOCATION/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf`
6. Edit the `BizEditorBundle.xlf` file in the following manner:

   a. Search for the following text:

   ```xml
   <file source-language="en" original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf" datatype="x-oracle-adf">
   
   <file source-language="en" target-language="LANG_CODE" original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf" datatype="x-oracle-adf">
   
   In this text, replace LANG_CODE with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

   ```xml
   <file source-language="en" target-language="ja" original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf" datatype="x-oracle-adf">
   
   c. Search for the application instance code. This procedure shows a sample edit for CRM On Demand application instance. The original code is:

   ```xml
   <trans-unit id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']"['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use rE0.UD_CRMOD_U_LANGUAGE_c_description']}">
   <source>Language</source>
   </target>
   </trans-unit>
   ```
2.4 Postcloning Steps

You can clone the connector by setting new names for some of the objects that comprise the connector. The outcome of the process is a new connector XML file. Most of the connector objects, such as Resource Object, Process Definition, Process Form, IT Resource Type Definition, IT Resource Instances, Lookup Definitions, Adapters, Reconciliation Rules and so on in the new connector XML file have new names.

See Also: The "Managing Connector Lifecycle" chapter of Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager for detailed information about cloning connectors and the steps mentioned in this section.

After a copy of the connector is created by setting new names for connector objects, some objects might contain the details of the old connector objects. Therefore, you must modify the following Oracle Identity Manager objects to replace the base...
connector artifacts or attribute references with the corresponding cloned artifacts or attributes:

- **Lookup Definition**
  
  If the lookup definition contains the old lookup definition details, then you must modify it to provide the new cloned lookup definition names. If the Code Key and Decode values are referring the base connector attribute references, then replace these with new cloned attributes.

- **Scheduled Job**
  
  You must replace the base connector resource object name in the scheduled job with the cloned resource object name. If the scheduled job parameter has any data referring to the base connector artifacts or attributes, then these must be replaced with the new cloned connector artifacts or attributes.

- **Localization Properties**
  
  You must update the resource bundle of a user locale with new names of the process form attributes for proper translations after cloning the connector. You can modify the properties file of your locale in the resources directory of the connector bundle.

  For example, the process form attributes are referenced in the Japanese properties file, CRMOD_ja.properties, as `global.udf.UD_CRMOD_ALIASNAME`. During cloning, if you change the process form name from `UD_CRMOD_U` to `UD_CRMOD1_U`, then you must update the process form attributes to `global.udf.UD_CRMOD1_ALIASNAME`. 
After you deploy the connector, you must configure it to meet your requirements. This chapter discusses the following connector configuration procedures:

- Section 3.1, "Configuring Reconciliation"
- Section 3.2, "Scheduled Jobs"
- Section 3.3, "Configuring Provisioning in Oracle Identity Manager Release 11.1.1"
- Section 3.4, "Configuring Provisioning in Oracle Identity Manager Release 11.1.2"

### 3.1 Configuring Reconciliation

Reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system, designated as a target resource.

By default, user accounts are reconciled in batches of 50 records. The maximum batch size permitted by Oracle CRM On Demand is 100. To change the batch size, you can specify a value for the Batch Size attribute of the reconciliation scheduled job. If you provide a batch size greater than 100, then the connector considers the Batch Size as 100. See Section 3.2.3, "Configuring Scheduled Jobs" for instructions to specify a value for this attribute.

During a reconciliation run:

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

This section discusses the following topics related to configuring reconciliation:

- Section 3.1.1, "Full Reconciliation"
- Section 3.1.2, "Limited Reconciliation"
- Section 3.1.3, "Reconciliation Rule for Target Resource Reconciliation"
- Section 3.1.4, "Reconciliation Action Rules for Target Resource Reconciliation"
3.1.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

To perform a full reconciliation run, remove (delete) any values currently assigned to the Filter and the Latest Token attributes of the CRM On Demand User Target Reconciliation scheduled job. See Section 3.2.2, "Scheduled Job for Reconciliation" for information about this scheduled job.

3.1.2 Limited Reconciliation

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

The connector provides a Filter attribute that allows you to use any of the Oracle CRM On Demand resource attributes to filter the target system records. You can use any of the values specified in the Decode column of the Lookup.CRMOD.UM.ReconAttrMap lookup definition. See Section 2.3.6.2, "Lookup.CRMOD.UM.ReconAttrMap" for more information.

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 Oracle CRM On Demand resource attributes to filter the target system records.

For detailed information about ICF Filters, see the "ICF Filter Syntax" section of the Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager.

While deploying the connector, follow the instructions in Section 3.2.3, "Configuring Scheduled Jobs" to specify attribute values.

3.1.3 Reconciliation Rule for Target Resource Reconciliation

The following is the process-matching rule:

**Rule name:** CRMOD Recon Rule

**Rule element:** User Login Equals User Login Id

In this rule:

- User Login is the User Login for Oracle Identity Manager:
- User Login Id is the User Login for the target system.

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand Development Tools.

---

**Note:** Perform the following procedure only after the connector is deployed.
4. Search for CRMOD Recon Rule. Figure 3–1 shows the reconciliation rule for target resource reconciliation.

**Figure 3–1  Reconciliation Rule for Target Resource Reconciliation**

Table 3–1 lists the action rules for target resource reconciliation.

**Table 3–1  Action Rules for Target Resource Reconciliation**

<table>
<thead>
<tr>
<th>Rule Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No Matches Found</td>
<td>None</td>
</tr>
<tr>
<td>One Entity Match Found</td>
<td>Establish Link</td>
</tr>
<tr>
<td>One Process Match Found</td>
<td>Establish Link</td>
</tr>
</tbody>
</table>

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

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **CRM On Demand** 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.
3.2 Scheduled Jobs

When you run the Connector Installer or import the connector XML file, the following reconciliation scheduled jobs are automatically created in Oracle Identity Manager:

This section discusses the following topics related to scheduled jobs:

- Section 3.2.1, "Scheduled Job for Lookup Field Synchronization"
- Section 3.2.2, "Scheduled Job for Reconciliation"
- Section 3.2.3, "Configuring Scheduled Jobs"

3.2.1 Scheduled Job for Lookup Field Synchronization

The following scheduled job is used for lookup field synchronization:

- CRM On Demand Role Lookup Recon

This scheduled job is used to synchronize the roles available on the target system into the Lookup.CRMOD.Roles lookup definition.

You must specify values for the attributes described in Table 3–2 for this scheduled jobs. The procedure to configure a scheduled job is described later in the guide.

Table 3–2 Attributes of the Scheduled Job for Lookup Field Synchronization

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| Code Key Attribute | Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute)  
  Default value: __NAME__  
  **Note:** You must not change the value of this attribute. |
| Decode Attribute   | Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute)  
  Default value: __NAME__ |
| Filter             | Expression for filtering records that must be reconciled by the scheduled job  
  By default, the value of this attribute is empty.  
  Sample value: equalTo('__NAME__', 'Administrator')  
  See Section 3.1.2, "Limited Reconciliation" for the syntax of this expression. |
| IT Resource Name   | Name of the IT resource for the target system installation from which you want to reconcile user records  
  Default value: CRM On Demand |
| Lookup Name        | Name of the lookup definition that maps each lookup definition with the data source from which values must be fetched  
  Default value: Lookup.CRMOD.Roles |
| Object Type        | Type of object whose values must be synchronized  
  Default value: __ROLES__  
  **Note:** You must not change the value of this attribute. |

3.2.2 Scheduled Job for Reconciliation

The CRM On Demand User Target Reconciliation scheduled task is used to reconcile user data in the target resource (account management) mode of the connector.
Scheduled Jobs

Table 3–3 describes the attributes of the scheduled job.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Batch Size</td>
<td>Number of records that must be included in each batch</td>
</tr>
<tr>
<td></td>
<td>Default value: 50</td>
</tr>
<tr>
<td>Filter</td>
<td>Expression for filtering records that must be reconciled by the scheduled job</td>
</tr>
<tr>
<td></td>
<td>By default, the value of this attribute is empty.</td>
</tr>
<tr>
<td></td>
<td><strong>Sample value:</strong> equalTo('Alias','SEPT12USER1')</td>
</tr>
<tr>
<td></td>
<td>See Section 3.1.2, &quot;Limited Reconciliation&quot; for the syntax of this expression.</td>
</tr>
<tr>
<td>IT Resource Name</td>
<td>Name of the IT resource for the target system installation from which you want to reconcile user records</td>
</tr>
<tr>
<td></td>
<td>Default value: CRM On Demand</td>
</tr>
<tr>
<td>Latest Token</td>
<td>Time stamp in the long format of the maximum value for the ModifiedDate attribute of the user records on the target system</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not enter a value for this attribute. The reconciliation engine automatically enters a value for this attribute.</td>
</tr>
<tr>
<td></td>
<td>If you set this attribute to an empty value, then incremental reconciliation operations fetch all the records (perform full reconciliation).</td>
</tr>
<tr>
<td>Object Type</td>
<td>Type of object you want to reconcile</td>
</tr>
<tr>
<td></td>
<td>Default value: User</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not modify the value of this attribute.</td>
</tr>
<tr>
<td>Resource Object Name</td>
<td>Name of the resource object that is used for reconciliation</td>
</tr>
<tr>
<td></td>
<td>Default value: CRM On Demand</td>
</tr>
<tr>
<td>Scheduled Job Name</td>
<td>Name of the scheduled job</td>
</tr>
<tr>
<td></td>
<td>Default value: CRM On Demand User Target Reconciliation</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> For the scheduled job shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the job, then you can enter the unique name for that scheduled job as the value of this attribute.</td>
</tr>
</tbody>
</table>

3.2.3 Configuring Scheduled Jobs

To configure a scheduled job:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For 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.
   - For Oracle Identity Manager release 11.1.2.x:
     a. Log in to Oracle Identity System Administration.

Note: The scheduled job does not support reconciliation of deleted records.

Note: The scheduled job does not support reconciliation of deleted records.

Table 3–3 Attributes of the Scheduled Job for Reconciliation
b. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see the "Managing Sandboxes" section of Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager.

c. In the left pane, under System Management, click Scheduler.

2. Search for and open the scheduled job as follows:
   a. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click Search Scheduled Jobs.
   b. 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.

3. 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.

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

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

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

   Attributes of the scheduled job are discussed in Section 3.2.2, "Scheduled Job for Reconciliation."

5. 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.

3.3 Configuring Provisioning in Oracle Identity Manager Release 11.1.1

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

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based
provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.3.4, "Switching Between Request-Based Provisioning and Direct Provisioning."

The following are types of provisioning operations:

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

See Also: Oracle Fusion Middleware Users’s Guide for Oracle Identity Manager for information about the types of provisioning

This section discusses the following topics:

- Section 3.3.1, "Guidelines on Performing Provisioning Operations"
- Section 3.3.2, "Configuring Direct Provisioning"
- Section 3.3.3, "Configuring Request-Based Provisioning"
- Section 3.3.4, "Switching Between Request-Based Provisioning and Direct Provisioning"

### 3.3.1 Guidelines on Performing Provisioning Operations

The following are guidelines that you must apply while performing provisioning operations:

- Before you perform provisioning operations, lookup definitions must be synchronized with the lookup fields of the target system. In other words, run the scheduled jobs for lookup field synchronization before provisioning operations.
- The Reports To field on the process form expects values in the *FirstName LastName* format.
- Passwords for user accounts provisioned from Oracle Identity Manager must adhere to the password policy set in the target system.
- The character length of target system fields must be taken into account when specifying values for the corresponding Oracle Identity Manager fields.
- The connector uses the SetPasswordAPI method for provisioning user passwords. On Oracle CRM On Demand target system, suppose users A and B have the ability to set passwords. Then, user A does not have the ability to update the password of user B.

### 3.3.2 Configuring Direct Provisioning

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

In direct provisioning, the Oracle Identity Manager administrator uses the Administrative and User Console to create a target system account for a user.

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. On the Welcome to Identity Administration page, in the Users region, click Create User.
3. On the Create User page, enter values for the OIM User fields, and then click the save icon.

4. If you want to provision a target system account to an existing OIM User, then:
   - On the Welcome to Identity Administration page, search for the OIM User by selecting Users from the list on the left pane.
   - From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

5. On the user details page, click the Resources tab.

6. 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.

7. On the Step 1: Select a Resource page, select CRM On Demand from the list and then click Continue.


9. On the Step 5: Provide Process Data for User Details page, enter the details of the account that you want to create 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.

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

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

3.3.3 Configuring Request-Based Provisioning

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

The following are features of request-based provisioning:

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

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

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

The following sections discuss the steps to be performed to enable request-based provisioning:

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

- Section 3.3.3.1, "End User's Role in Request-Based Provisioning"
- Section 3.3.3.2, "Approver's Role in Request-Based Provisioning"
- Section 3.3.3.3, "Importing Request Datasets Using Deployment Manager"
Section 3.3.3.4, "Enabling the Auto Save Form Feature"

Section 3.3.3.5, "Running the PurgeCache Utility"

3.3.3.1 End User's Role in Request-Based Provisioning
The following steps are performed by the end user in a request-based provisioning operation:

See Also: Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager for detailed information about these steps

1. Log in to the Administrative and User Console.
2. On the Welcome page, click Advanced in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the Administration tab, and then click the Requests tab.
4. From the Actions menu on the left pane, select Create Request.
   The Select Request Template page is displayed.
5. From the Request Template list, select Provision Resource and click Next.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click Search. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the Available Users list, select the user to whom you want to provision the account.
   If you want to create a provisioning request for more than one user, then from the Available Users list, select users to whom you want to provision the account.
8. Click Move or Move All to include your selection in the Selected Users list, and then click Next.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select CRM On Demand, move it to the Selected Resources list, and then click Next.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click Next.
12. On the Justification page, you can specify values for the following fields, and then click Finish.
   ■ Effective Date
   ■ Justification
   On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the Request History tab.

3.3.3.2 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.

### 3.3.3.3 Importing Request Datasets Using Deployment Manager

**See Also:** Oracle Fusion Middleware Administrator’s Guide for Oracle Identity Manager for detailed information about importing objects from an XML file using the Deployment Manager

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

To import a request dataset XML file by using the Deployment Manager:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management.
   A dialog box for opening files is displayed.
4. Locate and open the request dataset XML file, CRMOD-Datasets.xml, which is in the xml directory of the installation media.
   Details of this XML file are shown on the **File Preview** page.
5. Click **Add File**.
   The Substitutions page is displayed.
6. Click **Next**.
   The Confirmation page is displayed.
7. Click **Import**.
8. Close the Deployment Manager dialog box.
   The request dataset is imported into Oracle Identity Manager.

### 3.3.3.4 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 **CRM On Demand** process definition.
4. Select the **Auto Save Form** check box.
5. Click the save icon.

3.3.3.5 Running the PurgeCache Utility
Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.9, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

3.3.4 Switching Between Request-Based Provisioning and Direct Provisioning

Note: It is assumed that you have performed the procedure described in Section 3.3.3, "Configuring Request-Based Provisioning."

To switch from request-based provisioning to direct provisioning:
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 CRM On Demand 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 CRM On Demand resource object.
   c. Deselect the Self Request Allowed check box.
   d. Click the save icon.

To switch from direct provisioning back to request-based provisioning:
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 CRM On Demand 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 CRM On Demand resource object.
   c. Select the Self Request Allowed check box.
   d. Click the save icon.
3.4 Configuring Provisioning in Oracle Identity Manager Release 11.1.2

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 Administrative and User console.
2. Create a user. See the "Managing Users" chapter in *Oracle Fusion Middleware User’s Guide for 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**.
   
   See **Section 2.3.1, "Configuring Oracle Identity Manager 11.1.2 or Later"** for related procedures.
5. Specify values for fields in the application form and then click **Ready to Submit**.
6. Click **Submit**.
7. If you want to provision a CRM On Demand User, then:
   a. On the Users page, search for the required user.
   b. On the user details page, click **Accounts**.
   c. Click the **Request Accounts** button.
   d. Search for the CRM On Demand application instance in the catalog search box and select it.
   e. Click **Add to Cart**.
   f. Click **Checkout**.
   g. Specify values for fields in the application form and then click **Ready to Submit**.
   h. Click **Submit**.

---
Extending the Functionality of the Connector

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

- Section 4.1, "Adding Custom Attributes for Target Resource Reconciliation"
- Section 4.2, "Adding Custom Attributes for Provisioning"
- Section 4.3, "Configuring Validation of Data During Reconciliation and Provisioning"
- Section 4.4, "Configuring Transformation of Data During User Reconciliation"
- Section 4.5, "Configuring Resource Exclusion Lists"

4.1 Adding Custom Attributes for Target Resource Reconciliation

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

To add a custom attribute, you must ensure that the corresponding attribute exists on the target system. If it does not exist, then you must first add the custom attribute on the target system. Contact an administrator for information about adding a custom attribute on the target system.

By default, the attributes listed in Section 1.5, "User Attributes for Target Resource Reconciliation and Provisioning" are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can also configure the connector to reconcile custom attributes or other user attributes that are not available out of the box (OOTB) with the connector.

For example, if Legal Entity is a custom attribute added to the user profile on the target system, then you can configure the connector to reconcile this attribute by performing the following steps:
Adding Custom Attributes for Target Resource Reconciliation

See Also: Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager for detailed instructions on performing the steps in this procedure

1. For the custom attribute, Legal Entity, determine the corresponding attribute name in User Generic WSDL.
   
   You can invoke the FieldManagementRead Admin Web Service API and get the value of **Generic Integration Tag** for the Legal Entity user attribute.
   
   For example, Generic Integration Tag = CustomText2

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

3. Create a new version of the process form as follows:
   
   a. Expand **Development Tools**.
   
   b. Double-click **Form Designer**.
   
   c. Search for and open the UD_CRMOD_U process form.
   
   d. Click **Create New Version**.
      
      On the Create a new version dialog box, enter a new version in the Label field, and then click the save icon.

4. Add the new field on the process form as follows:
   
   a. Click **Add**.
      
      A field is added to the list. Enter the details of the field.
      
      For example, if you are adding the Legal Entity field, enter **UD_CRMOD_U.LEGALENTITY** in the **Name** field and the remaining details of this field.
      
      To add boolean attributes, select **ComboBox** from the Field Type list and select **String** as the Variant Type.
      
      If you are adding boolean attributes, create a new lookup definition, for example, Lookup.CRMOD.AttributeName. Then, add the following entries to the lookup definition:

      | Code Key | Decode |
      |----------|--------|
      | Y        | Y      |
      | N        | N      |

      Open the UD_CRMOD_U process form and click **Properties**. Select the newly added property and click **Add Property**. Select **Property Name** as Lookup Code, and then enter the newly created lookup, Lookup.CRMOD.AttributeName as the property value.

   b. Click the save icon.

   c. To activate the newly created form, click **Make Version Active**.
      
      Figure 4-1 is a sample screenshot of the new version of process form.
Adding Custom Attributes for Target Resource Reconciliation

Extending the Functionality of the Connector

Figure 4–1  Adding a New Version of Process Form

5. Add the new field to the list of reconciliation fields in the resource object as follows:
   b. Double-click Resource Objects.
   c. Search for and open the CRM On Demand resource object.
   d. On the Object Reconciliation tab, click Add Field.
   e. In the Add Reconciliation Field dialog box, enter the details of this field.
      For example, enter Legal Entity in the Field Name field and select String from the Field Type list.
   f. Click the save icon.
   g. On the Resource Objects form, click Create Reconciliation Profile to create reconciliation profile that would include the newly added reconciliation field.

Figure 4–2 is a sample screenshot of the newly added reconciliation field.
6. Create an entry for the field in the lookup definition for reconciliation as follows:
   a. Expand **Administration**.
   b. Double-click **Lookup Definition**.
   c. Search for and open the **Lookup.CRMOD.UM.ReconAttrMap** lookup definition.
   d. Click **Add** and enter the Code Key and Decode values for the field.
      The Code Key value must be the Recon Field label name. The Decode value
      must be the name of the attribute in the User Generic WSDL.
      For example, enter **Legal Entity** in the **Code Key** field and then enter **CustomText2** in the **Decode** field.
   e. Click the save icon.
      **Figure 4-3** is a sample screenshot of the new entry added to the reconciliation lookup definition.
7. Create a reconciliation field mapping for the new field on the process form as follows:
   b. Double-click Process Definition.
   c. From the Process Definition table, select and open the CRM On Demand resource object.
   d. Click Reconciliation Field Mappings and then click Add Field Map.
   e. In the Field Name field, select the value for the field that you want to add. For example, select Legal Entity.
   f. In the Field Type field, select the type of the field that is prepopulated.
   g. Double-click the Process Data Field field.
      A list of process data columns is displayed. From the list, select the process data column corresponding to the process data field.
      For example, select Legal Entity [String] = UD_CRMOD_U_LEGALENTITY.
   h. Click the save icon.

8. If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.2, "Creating a New UI Form" and Section 2.3.1.6, "Updating an Existing Application Instance with a New Form" for the procedures.
4.2 Adding Custom Attributes for Provisioning

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

To add a custom attribute, you must ensure that the corresponding attribute exists on the target system. If it does not exist, then you must first add the custom attribute on the target system. Contact an administrator for information about adding a custom attribute on the target system.

By default, the attributes listed in Section 1.5, "User Attributes for Target Resource Reconciliation and Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can also configure the connector for provisioning after adding custom attributes or other user attributes that are not available out of the box (OOTB) with the connector.

For example, if Legal Entity is a custom attribute added to the user profile on the target system, then you can configure the connector to provision this attribute by performing the following steps:

**See Also:** Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for detailed instructions on performing the steps in this procedure

1. For the custom attribute, Legal Entity, determine the corresponding attribute name in User Generic WSDL.

You can invoke the FieldManagementRead Admin Web Service API and get the value of **Generic Integration Tag** for the Legal Entity user attribute.

For example, Generic Integration Tag = CustomText2

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

3. Create a new version of the process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Search for and open the UD_CRMOD_U process form.
   d. Click **Create New Version**.

      On the Create a new version dialog box, enter a new version in the Label field, and then click the save icon.

4. Add the new field on the process form as follows:
   a. Click **Add**.

      A field is added to the list. Enter the details of the field.

      For example, if you are adding the Legal Entity field, enter **UD_CRMOD_U_LEGALENTITY** in the **Name** field, **Legal Entity** in the **Label Name** field, and the remaining details of this field.

      If you are adding boolean attributes, select **ComboBox** from the Field Type list and select **String** as the Variant Type.
Then, create a new lookup definition, for example, Lookup.CRMOD.AttributeName. Then, add the following entries to the lookup definition:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

Open the UD_CRMOD_U process form and click Properties. Select the newly added property and click Add Property. Select Property Name as Lookup Code, and then enter the newly created lookup, Lookup.CRMOD.AttributeName as the property value.

b. Click the save icon.

c. To activate the newly created form, click Make Version Active.

Figure 4–4 is a sample screenshot of the new version of process form.

**Figure 4–4 Adding a New Version of Process Form**

5. Create an entry for the field in the lookup definition for provisioning as follows:

a. Expand Administration.

b. Double-click Lookup Definition.

c. Search for and open the Lookup.CRMOD.UM.ProvAttrMap lookup definition.

d. Click Add and enter the Code Key and Decode values for the field.

The Code Key value must be the form field label name. The Decode value must be the attribute name in the User Generic WSDL.
For example, enter Legal Entity in the Code Key field and then enter CustomText2 in the Decode field.

e. Click the save icon.

Figure 4–5 is a sample screenshot of the new entry added to the provisioning lookup definition.

**Figure 4–5 Adding an Entry to Provisioning Lookup**

6. If you are using Oracle Identity Manager release 11.1.2.x or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.3.1.2, "Creating a New UI Form" and Section 2.3.1.6, "Updating an Existing Application Instance with a New Form" for the procedures.

### 4.3 Configuring Validation of Data During Reconciliation and Provisioning

The Lookup.CRMOD.UM.ProvValidations and Lookup.CRMOD.UM.ReconValidations lookup definitions hold single-valued data to be validated during provisioning and reconciliation operations, respectively.

For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.
To configure validation of data:

1. Write code that implements the required validation logic in a Java class with a fully qualified domain name (FQDN), such as `org.identityconnectors.crm.mod.extension.CRMODValidator`. This validation class must implement the validate method. The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

   ```java
   package com.validationexample;

   import java.util.HashMap;
   public class MyValidator {
       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 in to the Design Console.
   3. Create one of the following new lookup definitions:
      - To configure validation of data for reconciliation:

Note: The Lookup.CRMOD.UM.ProvValidations and Lookup.CRMOD.UM.ReconValidations lookup definitions are optional and do not exist by default.

You must add these lookups as decode values to the Lookup.CRMOD.UM.Configuration lookup definition to enable exclusions during provisioning and reconciliation operations. See Section 2.3.5, "Setting up the Lookup Definition for User Operations" for more information.
Configuring Validation of Data During Reconciliation and Provisioning

- Lookup.CRMOD.UM.ReconValidations
  - To configure validation of data for provisioning:
    - Lookup.CRMOD.UM.ProvValidations

4. In the **Code Key** column, enter the resource object field name that you want to validate. For example, Alias.

5. In the **Decode** column, enter the class name. For example, org.identityconnectors.crmod.extension.CRMODValidator.

6. Save the changes to the lookup definition.

7. Search for and open the **Lookup.CRMOD.UM.Configuration** lookup definition.

8. In the **Code Key** column, enter one of the following entries:
   - To configure validation of data for reconciliation:
     - Recon Validation Lookup
   - To configure validation of data for provisioning:
     - Provisioning Validation Lookup

9. In the **Decode** column, enter one of the following entries:
   - To configure validation of data for reconciliation:
     - Lookup.CRMOD.UM.ReconValidations
   - To configure validation of data for provisioning:
     - Lookup.CRMOD.UM.ProvValidations

10. Save the changes to the lookup definition.

11. Create a JAR with the class and upload it to the Oracle Identity Manager database as follows:
    Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 7 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

    - For Microsoft Windows:
      `OIM_HOME/server/bin/UploadJars.bat`
    - For UNIX:
      `OIM_HOME/server/bin/UploadJars.sh`

    When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Select 1 as the value of the JAR type.

    **Note:** Before you use this utility, verify that the **WL_HOME** environment variable is set to the directory in which Oracle WebLogic Server is installed.

**See Also:** *Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager* for detailed information about the Upload JARs utility.
12. Run the PurgeCache utility to clear content related to request datasets from the server cache.

13. Perform reconciliation or provisioning to verify validation for the field, for example, Alias.

### 4.4 Configuring Transformation of Data During User Reconciliation

The Lookup.CRMOD.UM.ReconTransformations lookup definition holds single-valued user data to be transformed during reconciliation operations. For example, you can use First Name and Last Name values to create a value for the Full Name field in Oracle Identity Manager.

To configure transformation of single-valued user data fetched during reconciliation:

1. Write code that implements the required transformation logic in a Java class with a fully qualified domain name (FQDN), such as org.identityconnectors.crmod.extension.CRMODTransformation.

   This transformation class must implement the transform method. The following sample transformation class creates a value for the Full Name attribute by using values fetched from the First Name and Last Name attributes of the target system:

   ```java
   package com.transformationexample;

   import java.util.HashMap;

   public class MyTransformer {
       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.

4. In the **Code Key** column, enter the resource object field name you want to transform. For example, *Alias*.

5. In the **Decode** column, enter the class name. For example, `org.identityconnectors.crmod.extension.CRMODTransformation`.

6. Save the changes to the lookup definition.

7. Search for and open the **Lookup.CRMOD.UM.Configuration** lookup definition.

8. In the **Code Key** column, enter Recon Transformation Lookup.

9. In the **Decode** column, enter `Lookup.CRMOD.UM.ReconTransformations`.

10. Save the changes to the lookup definition.

11. Create a JAR with the class and upload it to the Oracle Identity Manager database as follows:

    Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 7 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

    ```
    Note: Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.
    ```

    For Microsoft Windows:

    `OIM_HOME/server/bin/UploadJars.bat`

    For UNIX:

    `OIM_HOME/server/bin/UploadJars.sh`

    When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Select 1 as the value of the JAR type.

    **See Also:** Oracle Fusion Middleware Developer’s Guide for Oracle Identity Manager for detailed information about the Upload JARs utility

12. Run the PurgeCache utility to clear content related to request datasets from the server cache.

13. Perform reconciliation to verify transformation of the field, for example, *Alias*.

### 4.5 Configuring Resource Exclusion Lists

The **Lookup.CRMOD.UM.ProvExclusionList** and **Lookup.CRMOD.UM.ReconExclusionList** lookup definitions hold user IDs of target system accounts for which you do not want to perform provisioning and reconciliation operations, respectively.
Configuring Resource Exclusion Lists

The following is the format of the values stored in these lookups:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
<th>Sample Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login Id resource object field name</td>
<td>User ID of a user</td>
<td>Code Key: User Login Id</td>
</tr>
<tr>
<td></td>
<td>Decode: User001</td>
<td></td>
</tr>
<tr>
<td>User Login Id resource object field name with the [PATTERN] suffix</td>
<td>A regular expression supported by the representation in the java.util.regex.Pattern class</td>
<td>Code Key: User Login Id[PATTERN]</td>
</tr>
<tr>
<td></td>
<td>To exclude users matching any of the user ID's User001, User002, User088, then:</td>
<td>Decode: User001</td>
</tr>
<tr>
<td></td>
<td>To exclude users whose user ID's start with 00012, then:</td>
<td>Decode: 00012*</td>
</tr>
<tr>
<td></td>
<td>See Also: For information about the supported patterns, visit <a href="http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html">http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html</a></td>
<td></td>
</tr>
</tbody>
</table>

To add entries in the lookup for exclusions during provisioning operations:

1. On the Design Console, expand Administration and then double-click Lookup Definition.
2. Create a new lookup definition, Lookup.CRMOD.UM.ProvExclusionList.

   **Note:** To specify user IDs to be excluded during reconciliation operations, create a new lookup definition called Lookup.CRMOD.UM.ReconExclusionList and add entries to that lookup.

3. Click Add.
4. In the Code Key and Decode columns, enter the first user ID to exclude.

   **Note:** The Code Key represents the resource object field name on which the exclusion list is applied during provisioning operations.

5. Repeat Steps 3 and 4 for the remaining user IDs to exclude.

   For example, if you do not want to provision users with user IDs User001, User002, and User088 then you must populate the lookup definition with the following values:
You can also perform pattern matching to exclude user accounts. You can specify regular expressions supported by the representation in the java.util.regex.Pattern class.

**See Also:** For information about the supported patterns, visit [http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html](http://download.oracle.com/javase/6/docs/api/java/util/regex/Pattern.html)

For example, if you do not want to provision users matching any of the user IDs User001, User002, and User088, then you must populate the lookup definition with the following values:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login Id</td>
<td>User001</td>
</tr>
<tr>
<td>User Login Id</td>
<td>User002</td>
</tr>
<tr>
<td>User Login Id</td>
<td>User088</td>
</tr>
</tbody>
</table>

If you do not want to provision users whose user IDs start with 00012, then you must populate the lookup definition with the following values:

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login Id [PATTERN]</td>
<td>User001</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code Key</th>
<th>Decode</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Login Id [PATTERN]</td>
<td>00012*</td>
</tr>
</tbody>
</table>

6. Click the save icon.
The following is a known issue associated with this release of the connector:

- **Bug 14037345**

  The Reports To field on the process form does not provide an option to choose a manager for a user. If there are multiple managers on the target system with the same FirstName and LastName values, there may be a conflict when the connector tries to assign the correct manager for the user.
## Index

### C
- certified components, 1-1
- changing input locale, 2-6, 2-20
- clearing server cache, 2-20
- configuring
  - Oracle Identity Manager server, 2-6
  - configuring connector, 3-1
  - connector
    - features, 1-6
    - user attributes, 1-8
  - connector cloning, 2-22
  - connector configuration, 3-1
  - connector files and directories
    - description, 2-1
- Connector Installer, 2-4
- connector server, 2-5
- connector XML files, 2-2
- custom attributes
  - provisioning, 4-6
  - reconciliation, 4-1

### D
- deployment manager, 3-10
- direct provisioning, 3-7

### E
- enabling logging, 2-17
- exclusion lists, 4-12

### F
- files and directories of the connector
  - See connector files and directories
- Filter parameter, 3-2
- filtered reconciliation, 3-2
- filtering
  - target system records, 3-2

### G
- globalization features, 1-2

### I
- input locale, changing, 2-6, 2-20
- installing connector, 2-3, 2-4
- issues, 5-1
- IT resource
  - configuring for Connector Server, 2-11
  - configuring for target system, 2-9

### L
- limitations, 5-1
- limited reconciliation, 3-2
- logging enabling, 2-17
- lookup definition
  - Lookup.Configuration.CRMOD, 2-13
  - Lookup.CRMOD.Roles, 3-4
- lookup definitions
  - attribute mappings, 2-15
  - user operations, 2-14
  - lookup field synchronization, 2-15, 3-4
  - lookup fields, 2-15, 3-4

### M
- multilanguage support, 1-2

### O
- Oracle Identity Manager server, configuring, 2-6

### P
- provisioning, 3-6, 3-12
  - direct provisioning, 3-7
  - guidelines, 3-7
  - process, 1-5
  - provisioning triggered by policy changes, 3-7
  - request-based provisioning, 3-7
  - user attributes, 1-8
  - provisioning functions, 1-5

### R
- reconciliation
  - custom attributes, 4-1
  - full, 3-2
limited, 3-2
process, 1-4
scheduled jobs, 3-4
user attributes, 1-8
reconciliation rule
  target resource reconciliation, 3-2
request datasets
  importing, 3-10
request-based provisioning, 3-8

S
scheduled jobs, 3-4
server cache, clearing, 2-20
supported
  languages, 1-2
  releases of Oracle Identity Manager, 1-2
  target systems, 1-2

T
target resource reconciliation
  reconciliation action rules, 3-3
  reconciliation rule, 3-2
  target systems supported, 1-2
transformation, 4-11

V
validation, 4-8

X
xml files, 2-2