

Oracle® Identity Manager

Connector Guide for Oracle CRM On Demand



Release 11.1.1
E35136-08
June 2020

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

ORACLE®

Oracle Identity Manager Connector Guide for Oracle CRM On Demand, Release 11.1.1

E35136-08

Copyright © 2014, 2020, Oracle and/or its affiliates.

Primary Author: Gowri.G.R

Contributing Authors: Alankrita Prakash

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

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

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

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

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

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

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

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

Contents

Preface

Audience	viii
Documentation Accessibility	viii
Related Documents	viii
Conventions	viii

What's New in Oracle Identity Manager Connector for Oracle CRM On Demand?

Software Updates	x
Documentation-Specific Updates	x

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	1-6
1.4	Features of the Connector	1-6
1.4.1	ICF Based Connector	1-7
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	1-8
1.4.8	Support for Resource Exclusion Lists	1-8
1.5	User Attributes for Target Resource Reconciliation and Provisioning	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
2.1.3	Configuring the IBM Websphere to Import SSL Certificates from Target System	2-3
2.2	Installation	2-3
2.2.1	Installing the Connector in Oracle Identity Manager	2-4
2.2.2	Deploying the Connector Bundle in a Connector Server	2-5
2.3	Postinstallation	2-7
2.3.1	Configuring Oracle Identity Manager 11.1.2 or Later	2-7
2.3.1.1	Creating and Activating a Sandbox	2-7
2.3.1.2	Creating a New UI Form	2-8
2.3.1.3	Creating an Application Instance	2-8
2.3.1.4	Publishing a Sandbox	2-8
2.3.1.5	Syncing Catalog	2-9
2.3.1.6	Updating an Existing Application Instance with a New Form	2-9
2.3.1.7	Configuring Form Fields	2-9
2.3.2	Configuring the IT Resource for the Target System	2-10
2.3.3	Configuring the IT Resource for the Connector Server	2-12
2.3.4	Setting up the Lookup Definition for Connector Configuration	2-14
2.3.5	Setting up the Lookup Definition for User Operations	2-14
2.3.6	Setting up the Lookup Definitions for Attribute Mappings	2-16
2.3.6.1	Lookup.CRMOD.UM.ProvAttrMap	2-16
2.3.6.2	Lookup.CRMOD.UM.ReconAttrMap	2-17
2.3.6.3	Lookup.CRMOD.Roles	2-18
2.3.6.4	Lookup.CRMOD.Languages	2-18
2.3.7	Managing Logging	2-18
2.3.7.1	Understanding Log Levels	2-18
2.3.7.2	Enabling logging	2-19
2.3.8	Changing to the Required Input Locale	2-21
2.3.9	Clearing Content Related to Connector Resource Bundles from the Server Cache	2-21
2.3.10	Localizing Field Labels in UI Forms	2-22
2.4	Postcloning Steps	2-23

3 Using the Connector

3.1	Configuring Reconciliation	3-1
3.1.1	Performing Full Reconciliation	3-2
3.1.2	Performing Limited Reconciliation	3-2

3.1.3	Reconciliation Rule for Target Resource Reconciliation	3-2
3.1.3.1	Target Resource Reconciliation Rule	3-2
3.1.3.2	Viewing Target Resource Reconciliation Rule	3-3
3.1.4	Reconciliation Action Rules for Target Resource Reconciliation	3-3
3.1.4.1	Target Resource Reconciliation Action Rules	3-3
3.1.4.2	Viewing Target Resource Reconciliation Action Rules	3-4
3.2	Scheduled Jobs	3-4
3.2.1	Scheduled Job for Lookup Field Synchronization	3-4
3.2.2	Scheduled Job for Reconciliation	3-5
3.2.3	Configuring Scheduled Jobs	3-6
3.3	Configuring Provisioning in Oracle Identity Manager Release 11.1.1	3-7
3.3.1	Guidelines on Performing Provisioning Operations	3-8
3.3.2	Configuring Direct Provisioning	3-8
3.3.3	Configuring Request-Based Provisioning	3-9
3.3.3.1	End User's Role in Request-Based Provisioning	3-10
3.3.3.2	Approver's Role in Request-Based Provisioning	3-11
3.3.3.3	Importing Request Datasets Using Deployment Manager	3-11
3.3.3.4	Enabling the Auto Save Form Feature	3-12
3.3.3.5	Running the PurgeCache Utility	3-12
3.3.4	Switching Between Request-Based Provisioning and Direct Provisioning	3-12
3.3.4.1	Switching From Request-Based Provisioning to Direct Provisioning	3-12
3.3.4.2	Switching From Direct Provisioning to Request-Based Provisioning	3-13
3.4	Configuring Provisioning in Oracle Identity Manager Release 11.1.2	3-13

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	4-13

5 Known Issues

Index

List of Figures

1-1	Architecture of the Connector	1-3
2-1	Manage IT Resource Page	2-11
2-2	Edit IT Resource Details and Parameters Page	2-11
2-3	Manage IT Resource Page for Connector Server IT Resource	2-13
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

List of Tables

1-1	Certified Components	1-1
1-2	Provisioning Functions	1-6
1-3	User Attributes for Target Resource Reconciliation and Provisioning	1-8
2-1	Files and Directories On the Connector Installation Media	2-1
2-2	Parameters of the CRM On Demand IT Resource for the Target System	2-11
2-3	Parameters of the CRM On Demand Connector Server IT Resource	2-13
2-4	Entries in the Lookup.Configuration.CRMOD Lookup Definition	2-14
2-5	Entries in the Lookup.CRMOD.UM.Configuration	2-15
2-6	Entries in Lookup.CRMOD.UM.ProvAttrMap	2-16
2-7	Entries in Lookup.CRMOD.UM.ReconAttrMap	2-17
2-8	Log Levels and ODL Message Type:Level Combinations	2-19
3-1	Action Rules for Target Resource Reconciliation	3-4
3-2	Attributes of the Scheduled Job for Lookup Field Synchronization	3-5
3-3	Attributes of the Scheduled Job for Reconciliation	3-5

Preface

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, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E52734_01/index.html

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

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

Conventions

The following text conventions are used in this document:

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

Convention	Meaning
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that displays on the screen, or text that you enter.

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 [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 "8" of this guide:

- The "Oracle Identity Governance or Oracle Identity Manager" row in [Table 1-1](#) has been modified to include support for Oracle Identity Governance release 12c PS4 (12.2.1.4.0).

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

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

- The "Connector Server" row has been added to [Table 1-1](#).
- The "JDK" row of [Table 1-1](#) has been renamed to "Connector Server JDK".

The following is a documentation-specific update in revision "6" of this guide:

The "Oracle Identity Manager" row of [Table 1-1](#) 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 [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 [Performing Limited Reconciliation](#).

The following are documentation-specific updates in revision "3" of this guide:

- The "Oracle Identity Manager" row in [Table 1-1](#) has been modified.
- A note has been added in the "xml/CRMOD-Datasets.xml" row of [Table 2-1](#).
- The following sections have been added:
 - [Configuring Oracle Identity Manager 11.1.2 or Later](#)
 - [Localizing Field Labels in UI Forms](#)
 - [Configuring Provisioning in Oracle Identity Manager Release 11.1.1](#)
 - [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:
 - [Installing the Connector in Oracle Identity Manager](#)
 - [Configuring the IT Resource for the Target System](#)
 - [Configuring the IT Resource for the Connector Server](#)
 - [Configuring Scheduled Jobs](#)

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to 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:

- [Certified Components](#)
- [Certified Languages](#)
- [Connector Architecture](#)
- [Features of the Connector](#)
- [User Attributes for Target Resource Reconciliation and Provisioning](#)

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.

Table 1-1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: <ul style="list-style-type: none">• Oracle Identity Governance release 12c (12.2.1.4.0)• Oracle Identity Governance release 12c (12.2.1.3.0)• Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)• Oracle Identity Manager 11g Release 2 BP04 (11.1.2.0.4) and any later BP in this release track• Oracle Identity Manager 11g Release 1 BP01 (11.1.1.5.1) and any later BP in this release track
Target systems	Oracle CRM On Demand Release 19 or later
Connector Server	11.1.2.1.0

Table 1-1 (Cont.) Certified Components

Item	Requirement
Connector Server JDK	JDK 1.6 Update 24 or later, or JRockit JDK 1.6 Update 24 or later

1.2 Certified Languages

The connector supports the following languages:

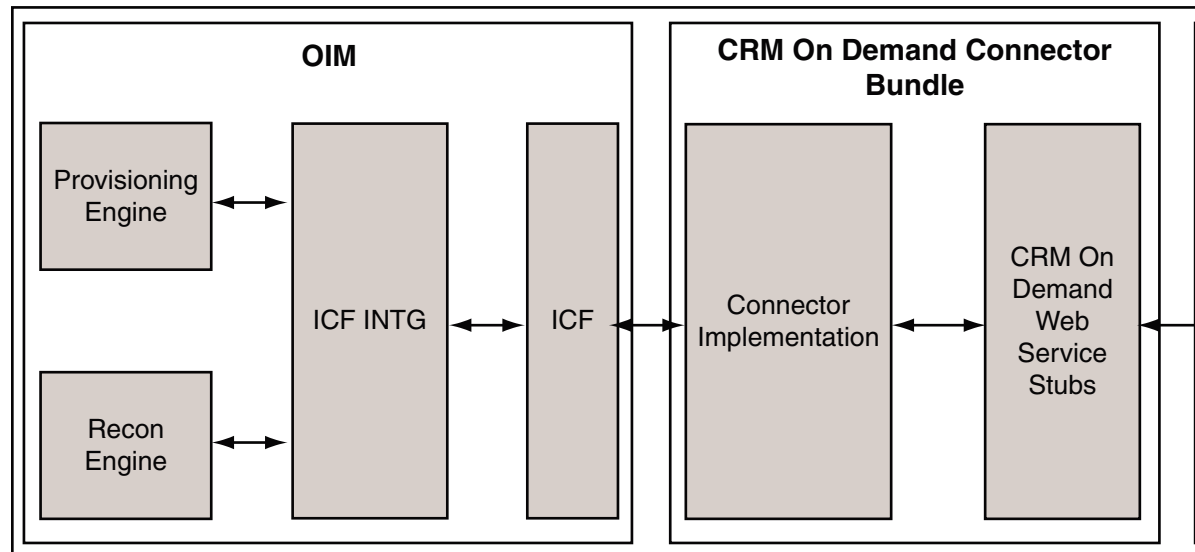
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

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). In 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:

- [Reconciliation Process](#)
- [Provisioning Process](#)
- [Provisioning Functions](#)

1.3.1 Reconciliation Process

See Also:

Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about Reconciliation

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.

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 [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

See Also:

Managing Provisioning Tasks in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for conceptual information about Provisioning

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 1-2 Provisioning Functions

Function	Adapter
Create User	CRMODCreateUser
Delete User	CRMODDisableUser
Disable User	CRMODDisableUser
Enable User	CRMODEnableUser
Alias Updated	CRMODUpdateUser
Cell Phone Updated	CRMODUpdateUser
Department Updated	CRMODUpdateUser
Division Updated	CRMODUpdateUser
Email Updated	CRMODUpdateUser
Employee Number Updated	CRMODUpdateUser
External Unique ID Updated	CRMODUpdateUser
First Name Updated	CRMODUpdateUser
Job Title Updated	CRMODUpdateUser
Language Updated	CRMODUpdateUser
Last Name Updated	CRMODUpdateUser
Middle Name Updated	CRMODUpdateUser
Password Updated	CRMODUpdateUser
Region Updated	CRMODUpdateUser
Reports To Updated	CRMODUpdateUser
Role Updated	CRMODUpdateUser
Work Phone Updated	CRMODUpdateUser

1.4 Features of the Connector

- [ICF Based Connector](#)
- [Support for Target Resource Reconciliation](#)
- [Support for Both Full and Incremental Reconciliation](#)
- [Support for Limited Reconciliation](#)
- [Support for Adding Custom Attributes for Reconciliation and Provisioning](#)
- [Support for Transformation of Data](#)
- [Support for Validation of Data](#)
- [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 Understanding the Identity Connector Framework in *Oracle Fusion Middleware Developing and Customizing Applications 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 [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 [Performing 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 [Performing 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 [Adding Custom Attributes for Target Resource Reconciliation](#) and [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 [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 [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.

[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 1-3 User Attributes for Target Resource Reconciliation and Provisioning

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

2

Deploying the Connector

The procedure to deploy the connector can be divided into these stages.

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

2.1 Preinstallation

Preinstallation involves understanding the files available in the connector installation media, configuring JSEE-based SSL, and so on.

- [Files and Directories on the Installation Media](#)
- [Configuring the Oracle WebLogic Server to Use JSSE-based SSL](#)
- [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 2-1 Files and Directories On the Connector Installation Media

File in the Installation Media Directory	Description
bundle/org.identityconnectors.crmmod-1.0.0001	This JAR file contains the connector bundle.
configuration/CRMOD-CI.xml	This XML file contains configuration information that is used during the connector installation process.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to Oracle Identity Manager database. Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.

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

File in the Installation Media Directory	Description
xml/CRMOD-ConnectorConfig.xml	<p>This XML file contains definitions for the connector components. These components include the following:</p> <ul style="list-style-type: none"> • IT resource type • Process form • Process task and adapters (along with their mappings) • Resource object • Provisioning process • Prepopulate rules • Lookup definitions • Scheduled jobs
xml/CRMOD-Datasets.xml	<p>This XML file contains request datasets that can be imported using Deployment Manager. It specifies the information to be submitted by the requester during a request-based provisioning operation.</p> <p>See Importing Request Datasets Using Deployment Manager for more information.</p> <p>Note: Use this file only if you are using Oracle Identity Manager release prior to 11.1.2.</p>

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.



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.

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.

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:

Field Name	Field Value	Host
Name	secure-ausomxdsa.crmondemand.com	Port 443
Alias	ecure-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 [Installing the Connector in Oracle Identity Manager](#).

- To run the connector code remotely in a Connector Server, perform the procedures described in [Installing the Connector in Oracle Identity Manager](#) and [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/server/ConnectorDefaultDirectory
2. If you are using Oracle Identity Manager release 11.1.1, then perform the following steps:
 - a. Log in to the Administrative and User Console.
 - b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.
3. If you are using Oracle Identity Manager release 11.1.2.x, then perform the following steps:
 - a. Log in to Oracle Identity System Administration.
 - b. In the left pane, under System Management, click **Manage Connector**.
4. In the Manage Connector page, click **Install**.
5. From the Connector List list, select **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**.
6. Click **Load**.
7. To start the installation process, click **Continue**.

The following tasks are performed, in sequence:

- a. Configuration of connector libraries

- b. Import of the connector 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.
8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. 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 [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 [Installing the Connector in Oracle Identity Manager](#).

 **Note:**

- You can download the Connector Server from the Oracle Technology Network web page.
- See [Configuring the IT Resource for the Connector Server](#) for related information.
- See Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications 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`:

- a. `ORACLE_COMMON/webservices/wsclient_extended.jar`
- b. `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"
```

6. Start the Connector Server.

2.3 Postinstallation

Postinstallation involves performing certain procedures such as configuring Oracle Identity Manager, configuring the IT resource for the target system and Connector Server, enabling logging, localizing field labels, and so on.

- [Configuring Oracle Identity Manager 11.1.2 or Later](#)
- [Configuring the IT Resource for the Target System](#)
- [Configuring the IT Resource for the Connector Server](#)
- [Setting up the Lookup Definition for Connector Configuration](#)
- [Setting up the Lookup Definition for User Operations](#)
- [Setting up the Lookup Definitions for Attribute Mappings](#)
- [Managing Logging](#)
- [Changing to the Required Input Locale](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [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:

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Creating an Application Instance](#)
- [Publishing a Sandbox](#)
- [Syncing Catalog](#)
- [Updating an Existing Application Instance with a New Form](#)
- [Configuring Form Fields](#)

2.3.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see [Managing Sandboxes](#) in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes**. The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox**. The Create Sandbox dialog box is displayed.

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

2.3.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see *Managing Forms in Oracle Fusion Middleware Administering 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 *Managing Application Instances in Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances**.
2. Under Search Results, click **Create**.
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save**.

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 [Creating and Activating a Sandbox](#):

1. Close all the open tabs and pages.

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

2.3.1.5 Syncing Catalog

To sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in [Scheduled Job for Lookup Field Synchronization](#).
2. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.3.1.6 Updating an Existing Application Instance with a New Form

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

1. Create a sandbox and activate it as described in [Creating and Activating a Sandbox](#).
2. Create a new UI form for the resource as described in [Creating a New UI Form](#).
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in [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 [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. If you are using Oracle Identity Manager release 11.1.1, then:
 - a. Log in to the Administrative and User Console.
 - b. On the Welcome page, click **Advanced** in the upper-right corner of the page.
 - c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
2. If you are using Oracle Identity Manager release 11.1.2.x, then log in to Oracle Identity System Administration, then in the left pane under Configuration, click **IT Resource**.
3. 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

4. Click the edit icon corresponding to the CRM On Demand IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. 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 2-2 Parameters of the CRM On Demand IT Resource for the Target System

Parameter	Description
Configuration Lookup	Name of the lookup definition that stores configuration information used during reconciliation and provisioning Default value: Lookup.Configuration.CRMOD

Table 2-2 (Cont.) Parameters of the CRM On Demand IT Resource for the Target System

Parameter	Description
Connector Server Name	Name of the IT resource of type "Connector Server" By default, this field is blank. Note: 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 Configuring the IT Resource for the Connector Server for information about modifying the IT resource attributes.
adminID	User ID of the administrator to perform connector operations Sample value: GPIANOSI13-19/JOHN.DOE
adminPassword	Password of the administrator
targetUrl	URL of the Oracle CRM On Demand target system. Note: The value of this field must not contain '/' (forward slash character) at the end.

- 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 [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:

- If you are using Oracle Identity Manager release 11.1.1, then:
 - Log in to the Administrative and User Console.
 - On the Welcome page, click **Advanced** in the upper-right corner of the page.
 - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
- If you are using Oracle Identity Manager release 11.1.2.x, then log in to Oracle Identity System Administration, then in the left pane under Configuration, click **IT Resource**.
- 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

4. Click the edit icon corresponding to the Connector Server IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the Connector Server IT resource. [Figure 2-4](#) shows the Edit IT Resource Details and Parameters page.

Figure 2-4 Edit IT Resource Details and Parameters Page for Connector Server IT Resource

[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

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the Connector Server. Sample value: HostName
Key	Enter the key for the Connector Server.

Table 2-3 (Cont.) Parameters of the CRM On Demand Connector Server IT Resource

Parameter	Description
Port	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
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the Connector Server and Oracle Identity Manager times out. If the value is zero or if no value is specified, the connection will not timeout. Recommended value: 0
UseSSL	Enter <code>yes</code> to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter <code>no</code> . Default value: <code>no</code>

- 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.CRMOD Lookup Definition

Code Key	Decode	Description
Bundle Name	<code>org.identityconnectors.crm</code>	Name of the connector bundle package Do not modify this entry.
Bundle Version	1.0.0001	Version of the connector bundle class Do not modify this entry.
Connector Name	<code>org.identityconnectors.crm</code> <code>.CRMConnector</code>	Name of the connector class Do not modify this entry.
User Configuration Lookup	<code>Lookup.CRM.UM.Configuration</code> <code>n</code>	Name of the lookup definition that contains user-specific configuration properties Do not modify this entry.

2.3.5 Setting up the Lookup Definition for User Operations

The `Lookup.CRM.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.CRMOD.UM.Configuration

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.CRMOD.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and attributes in User Generic WSDL. See Lookup.CRMOD.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.CRMOD.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and attributes in User Generic WSDL. See Lookup.CRMOD.UM.ReconAttrMap for more information about this lookup definition.
Recon Transformation Lookup	Lookup.CRMOD.UM.ReconTransformations	This entry holds the name of the lookup definition that is used to configure transformation of attribute values that are fetched from the target system during user reconciliation. See Configuring Transformation of Data During User Reconciliation for more information about adding entries in this lookup definition.
Provisioning Validation Lookup	Lookup.CRMOD.UM.ProvValidations	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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Recon Validation Lookup Note: This entry does not exist by default. You must add it if you want to enable transformation during reconciliation.	Lookup.CRMOD.UM.ReconValidation	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 Configuring Validation of Data During Reconciliation and Provisioning for more information about adding entries in this lookup definition.
Provisioning Exclusion Lookup Note: This entry does not exist by default. You must add it if you want to enable resource exclusions during reconciliation.	Lookup.CRMOD.UM.ProvExclusionList	This entry holds the name of the lookup definition that is used to configure resource exclusion lists during reconciliation. See Configuring Resource Exclusion Lists for more information.
Recon Exclusion Lookup Note: This entry does not exist by default. You must add it if you want to enable resource exclusions during provisioning.	Lookup.CRMOD.UM.ReconExclusionList	This entry holds the name of the lookup definition that is used to configure resource exclusion lists during provisioning operations. See Configuring Resource Exclusion Lists for more information about adding entries in this lookup definition.

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:

- [Lookup.CRMOD.UM.ProvAttrMap](#)
- [Lookup.CRMOD.UM.ReconAttrMap](#)
- [Lookup.CRMOD.Roles](#)
- [Lookup.CRMOD.Languages](#)

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 [Adding Custom Attributes for Provisioning](#) for more information.

[Table 2-6](#) lists the default entries in this lookup definition.

Table 2-6 Entries in Lookup.CRMOD.UM.ProvAttrMap

Code Key	Decode
Alias	Alias
Cell Phone	CellPhone
Department	Department
Division	Division
Email	EmailAddr
Employee Number	EmployeeNumber
External Unique ID	ExternalSystemId
First Name	FirstName
Job Title	JobTitle
Language	Language
Last Name	LastName
Middle Name	MiddleName
Password	__PASSWORD__
Region	Region
Reports To	ManagerFullName
Return ID	__UID__
Role[LOOKUP]	Role
User Login Id	UserLoginId

Table 2-6 (Cont.) Entries in Lookup.CRMOD.UM.ProvAttrMap

Code Key	Decode
Work Phone	PhoneNumber

2.3.6.2 Lookup.CRMOD.UM.ReconAttrMap

The Lookup.CRMOD.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 [Adding Custom Attributes for Target Resource Reconciliation](#) for more information.

[Table 2-7](#) lists the default entries in this lookup definition.

Table 2-7 Entries in Lookup.CRMOD.UM.ReconAttrMap

Code Key	Decode
Alias	Alias
Cell Phone	CellPhone
Department	Department
Division	Division
Email	EmailAddr
Employee Number	EmployeeNumber
External Unique ID	ExternalSystemId
First Name	FirstName
Job Title	JobTitle
Language	Language
Last Name	LastName
Middle Name	MiddleName
Region	Region
Reports To	ManagerFullName
Return ID	UserId
Role[LOOKUP]	Role
Show Welcome Page	ShowWelcomePage
Status	Status
User Login Id	UserLoginId
Work Phone	PhoneNumber

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:

Code Key	Decode
Chinese (Simplified)	Chinese (Simplified)
English-American	English-American
English-British	English-British
French	French
German	German
Italian	Italian
Japanese	Japanese
Korean	Korean
Portuguese	Portuguese
Spanish	Spanish

2.3.7 Managing Logging

Oracle Identity Manager uses the Oracle Diagnostic Logging (ODL) logging service for recording all types of events pertaining to the connector.

The following topics provide detailed information about logging:

- [Understanding Log Levels](#)
- [Enabling logging](#)

2.3.7.1 Understanding Log Levels

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:

- 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 2-8 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

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

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

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

2.3.7.2 Enabling logging

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]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
  <property name='logreader:' value='off' />
    <property name='path' value='[FILE_NAME]' />
    <property name='format' value='ODL-Text' />
    <property name='useThreadName' value='true' />
    <property name='locale' value='en' />
    <property name='maxFileSize' value='5242880' />
    <property name='maxLogSize' value='52428800' />
    <property name='encoding' value='UTF-8' />
  </log_handler>
```

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

- b. Replace both occurrences of [LOG_LEVEL] with the ODL message type and level combination that you require. Table 2-8 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="NOTIFICATION:1"
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.

2.3.10 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. The resource bundles are available in the connector installation media.



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:

```
<file source-language="en"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

- b. Replace with the following text:

```
<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:

```
<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:

```

<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_CRMOD_U_LANGUAGE__c_description']}">
<source>Language</source>
</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.CRMUserForm.entity.CRMUse
rFormEO.UD_CRMOD_U_LANGUAGE__c_LABEL">
<source>Language</source>
</target>
</trans-unit>

```

- d. Open the resource file from the connector package, for example `CRMOD_ja.properties`, and get the value of the attribute from the file, for example, `global.udf.UD_CRMOD_U_LANGUAGE=\u8A00\u8A9E`.
- e. Replace the original code shown in Step 6.c with the following:

```

<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundl
e']}
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.
UD_CRMOD_U_LANGUAGE__c_description']}">
<source>Language</source>
<target>\u8A00\u8A9E</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.CRMUserForm.entity.CRMUse
rFormEO.UD_CRMOD_U_LANGUAGE__c_LABEL">
<source>Language</source>
<target>\u8A00\u8A9E</target>
</trans-unit>

```

- f. Repeat Steps 6.a through 6.d for all attributes of the process form.
- g. Save the file as `BizEditorBundle_LANG_CODE.xlf`. In this file name, replace `LANG_CODE` with the code of the language to which you are localizing.
Sample file name: `BizEditorBundle_ja.xlf`.
7. Repackage the ZIP file and import it into MDS.

See Also:

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

8. Log out of and log in to Oracle Identity Manager.

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:

Cloning Connectors in *Oracle Fusion Middleware Administering 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`.

3

Using the Connector

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

This chapter discusses the following connector configuration procedures:

Note:

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

- [Configuring Reconciliation](#)
- [Scheduled Jobs](#)
- [Configuring Provisioning in Oracle Identity Manager Release 11.1.1](#)
- [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 [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:

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

3.1.1 Performing 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 [Scheduled Job for Reconciliation](#) for information about this scheduled job.

3.1.2 Performing Limited Reconciliation

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

The connector provides a Filter 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 [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 ICF Filter Syntax in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

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

3.1.3 Reconciliation Rule for Target Resource Reconciliation

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

- [Target Resource Reconciliation Rule](#)
- [Viewing Target Resource Reconciliation Rule](#)

3.1.3.1 Target Resource Reconciliation Rule

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.

3.1.3.2 Viewing Target Resource Reconciliation Rule

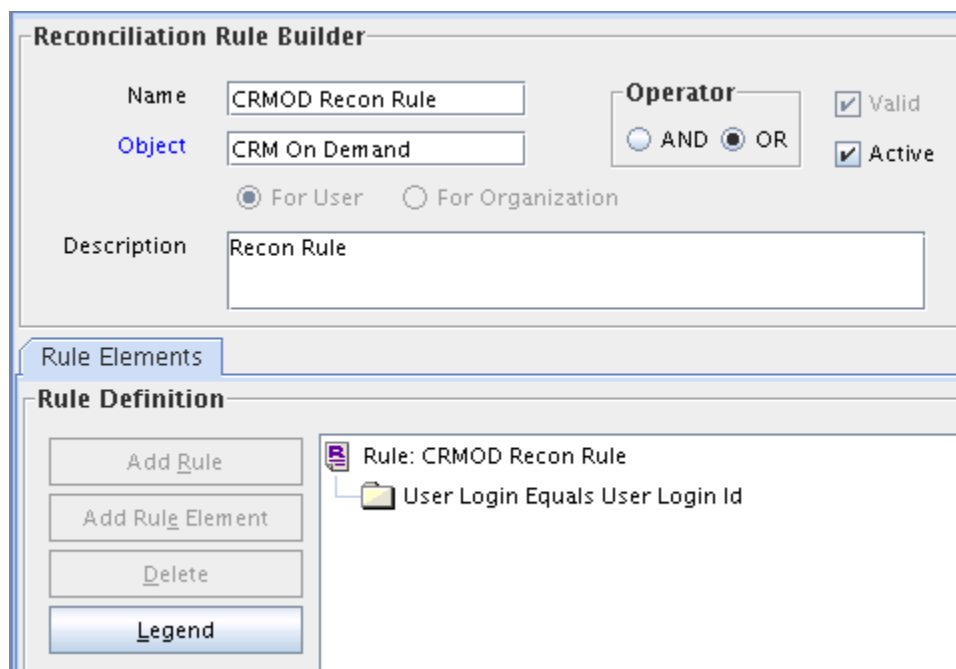
After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

 **Note:**

Perform the following procedure only after the connector is deployed.

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

Figure 3-1 Reconciliation Rule for Target Resource Reconciliation



Reconciliation Rule Builder

Name: CRMOD Recon Rule

Object: CRM On Demand

Operator: AND OR (OR selected)

Valid: Valid

Active: Active

For User: For User For Organization:

Description: Recon Rule

Rule Elements

Rule Definition

Add Rule

Add Rule Element

Delete

Legend

Rule: CRMOD Recon Rule

User Login Equals User Login Id

3.1.4 Reconciliation Action Rules for Target Resource Reconciliation

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

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

3.1.4.1 Target Resource Reconciliation Action Rules

[Table 3-1](#) lists the action rules for target resource reconciliation.

Table 3-1 Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

**Note:**

No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions.

3.1.4.2 Viewing Target Resource Reconciliation Action Rules

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **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:

- [Scheduled Job for Lookup Field Synchronization](#)
- [Scheduled Job for Reconciliation](#)
- [Configuring Scheduled Jobs](#)

3.2.1 Scheduled Job for Lookup Field Synchronization

The CRM On Demand Role Lookup Recon scheduled job is used for lookup field synchronization. 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

Attribute	Description
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: <code>__NAME__</code> 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: <code>__NAME__</code>
Filter	Expression for filtering records that must be reconciled by the scheduled job By default, the value of this attribute is empty. Sample value: <code>equalTo('__NAME__', 'Administrator')</code> See Performing 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: <code>CRM On Demand</code>
Lookup Name	Name of the lookup definition that maps each lookup definition with the data source from which values must be fetched Default value: <code>Lookup.CRMOD.Roles</code>
Object Type	Type of object whose values must be synchronized Default value: <code>__ROLES__</code> 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.

 **Note:**

The scheduled job does not support reconciliation of deleted records.

[Table 3-3](#) describes the attributes of the scheduled job.

Table 3-3 Attributes of the Scheduled Job for Reconciliation

Attribute	Description
Batch Size	Number of records that must be included in each batch Default value: 50

Table 3-3 (Cont.) Attributes of the Scheduled Job for Reconciliation

Attribute	Description
Filter	Expression for filtering records that must be reconciled by the scheduled job By default, the value of this attribute is empty. Sample value: <code>equalTo('Alias','SEPT12USER1')</code> See Performing 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
Latest Token	Time stamp in the long format of the maximum value for the ModifiedDate attribute of the user records on the target system Note: Do not enter a value for this attribute. The reconciliation engine automatically enters a value for this attribute. If you set this attribute to an empty value, then incremental reconciliation operations fetch all the records (perform full reconciliation).
Object Type	Type of object you want to reconcile Default value: User Note: Do <i>not</i> modify the value of this attribute.
Resource Object Name	Name of the resource object that is used for reconciliation Default value: CRM On Demand
Scheduled Job Name	Name of the scheduled job Default value: CRM On Demand User Target Reconciliation Note: 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.

3.2.3 Configuring Scheduled Jobs

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1, then:
 - 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.
2. If you are using Oracle Identity Manager release 11.1.2.x, then:
 - a. Log in to Oracle Identity System Administration.
 - b. Create and activate a sandbox. For detailed instructions on creating and activating a sandbox, see *Managing Sandboxes in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.
 - c. In the left pane, under System Management, click **Scheduler**.
3. 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.
 4. On the Job Details tab, you can modify the following parameters:

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

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

 **Note:**

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

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

5. 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 [Scheduled Job for Reconciliation](#).

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

 **Note:**

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

3.3 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 [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

This section discusses the following topics:

- [Guidelines on Performing Provisioning Operations](#)
- [Configuring Direct Provisioning](#)
- [Configuring Request-Based Provisioning](#)
- [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**.
8. On the Step 2: Verify Resource Selection page, 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.

- [End User's Role in Request-Based Provisioning](#)
- [Approver's Role in Request-Based Provisioning](#)
- [Importing Request Datasets Using Deployment Manager](#)
- [Enabling the Auto Save Form Feature](#)
- [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:

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:

Importing Using the Deployment Manager and Sandbox in *Oracle Fusion Middleware Administering 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 [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

If you have configured the connector for request-based provisioning, you can always switch to direct provisioning. Similarly, you can always switch back to request-based provisioning any time.



Note:

It is assumed that you have performed the procedure described in [Configuring Request-Based Provisioning](#).

This section discusses the following topics:

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

3.3.4.1 Switching From Request-Based Provisioning to Direct Provisioning

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

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

- a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **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.

3.3.4.2 Switching From Direct Provisioning to Request-Based Provisioning

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

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
 - a. Expand **Process Management**, and then double-click **Process Definition**.
 - b. Search for and open the **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 *Creating a User in Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts**.

4. In the Catalog page, search for and add to cart the application instance, and then click **Checkout**.
See [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**.

4

Extending the Functionality of the Connector

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

This chapter discusses the following connector configuration procedures:

Note:

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

- [Adding Custom Attributes for Target Resource Reconciliation](#)
- [Adding Custom Attributes for Provisioning](#)
- [Configuring Validation of Data During Reconciliation and Provisioning](#)
- [Configuring Transformation of Data During User Reconciliation](#)
- [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 [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:

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**.

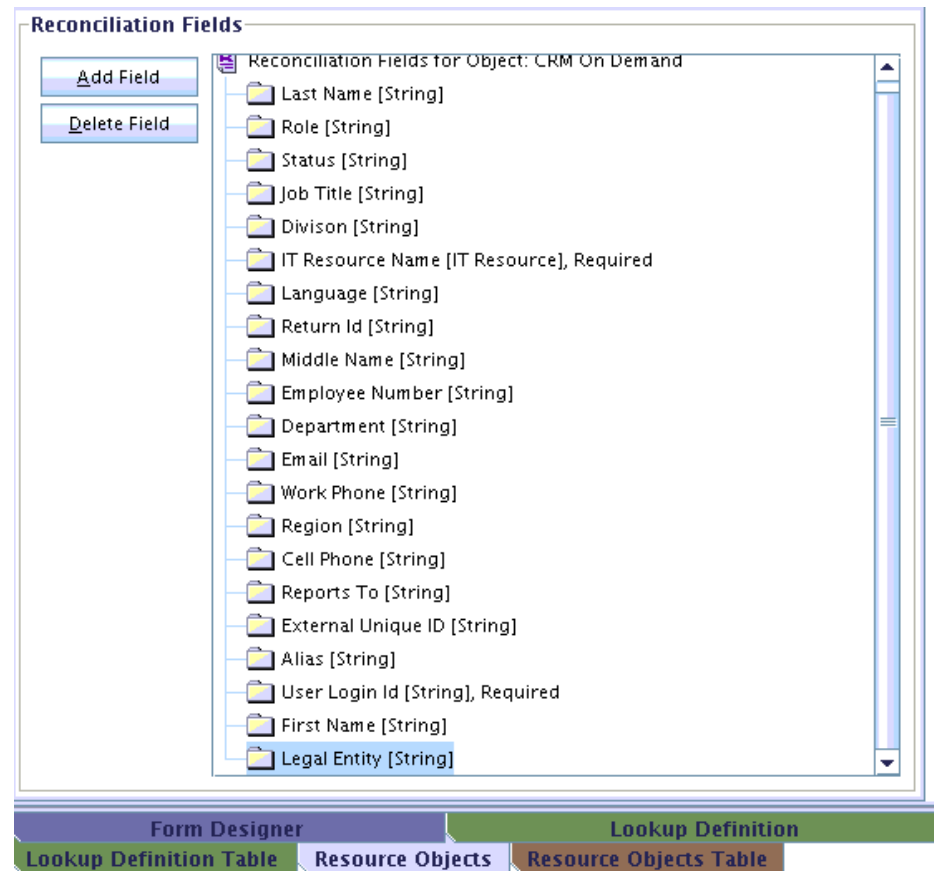
Figure 4-1 is a sample screenshot of the new version of process form.

Figure 4-1 Adding a New Version of Process Form

	Name	Variant Ty...	Len...	Field Label	Field Type
14	UD_CRMOD_U_DEPARTMENT	String	100	Department	TextField
15	UD_CRMOD_U_CELLPHONE	String	100	Cell Phone	TextField
16	UD_CRMOD_U_EMAIL	String	100	Email	TextField
17	UD_CRMOD_U_RETURNID	String	100	Return Id	DOField
18	UD_CRMOD_U_ROLE	String	100	Role	LookupField
19	UD_CRMOD_U_FIRSTNAME	String	100	First Name	TextField
20	UD_CRMOD_U_EMPLOYEEENO	String	100	Employee Number	TextField
21	UD_CRMOD_U_LANGUAGE	String	100	Language	LookupField
22	UD_CRMOD_U_LEGALENTITY	String	100	Legal Entity	TextField

5. Add the new field to the list of reconciliation fields in the resource object as follows:
 - a. Expand **Resource Management**.
 - 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.

Figure 4-2 Adding a New 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.

Figure 4-3 Adding an Entry to Reconciliation Lookup

Lookup Definition

Code:

Field:

Lookup Type Field Type

Required:

Group:

Lookup Code Information

	Code Key	Decode
4	Division	Division
5	Email	EmailAddr
6	Employee Number	EmployeeNumber
7	External Unique ID	ExternalSystemId
8	First Name	FirstName
9	Job Title	JobTitle
10	Language	Language
11	Last Name	LastName
12	Legal Entity	CustomText2
13	Middle Name	MiddleName
14	Region	Region
15	Reports To	ManagerFullName
16	Return Id	UserId
17	Role[LOOKUP]	Role
18	Show Welcome Page	ShowWelcomePage
19	Status	Status
20	User Login Id	UserLoginId
21	Work Phone	PhoneNumber

Form Designer | Lookup Definition | **Lookup Definition Table**

7. Create a reconciliation field mapping for the new field on the process form as follows:
 - a. Expand **Process Management**.
 - 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 [Creating a New UI Form](#) and [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 [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:

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:

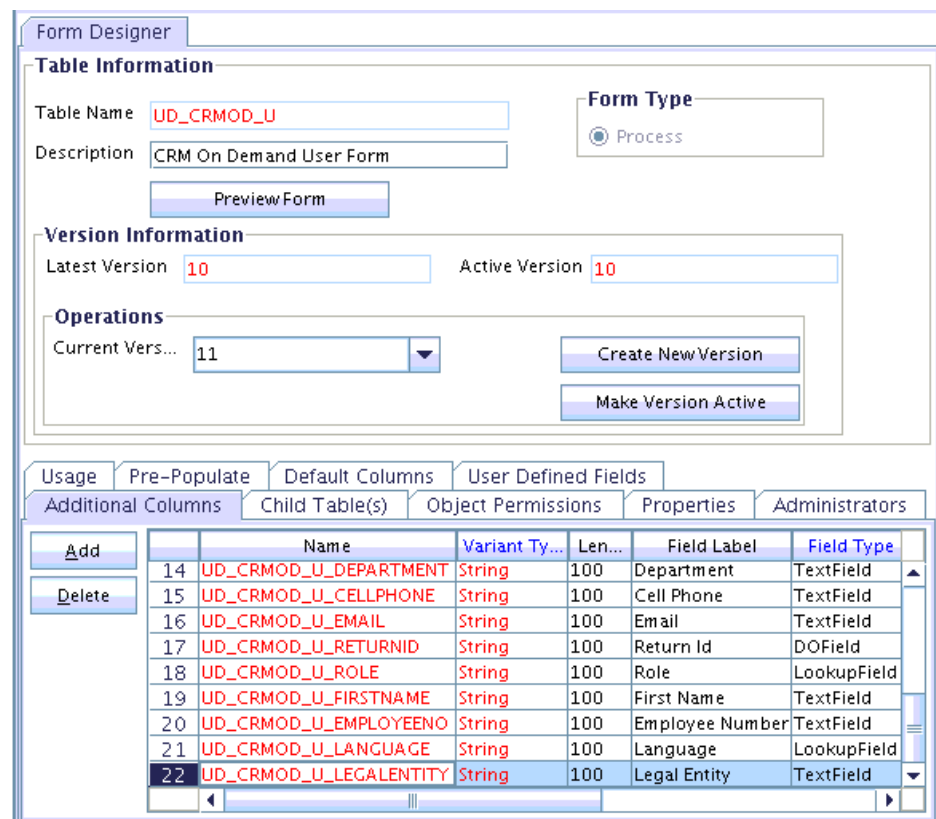
Code Key	Decode
Y	Y
N	N

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 4-4 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

The screenshot shows the 'Lookup Definition' form with the following fields:

- Code: `Lookup.CRMOD.UM.ProvAttrMap`
- Field: (empty)
- Lookup Type: (selected)
- Field Type:
- Required:
- Group: `CRMOD`

Below the form is the 'Lookup Code Information' table:

	Code Key	Decode
7	External Unique ID	ExternalSystemId
8	First Name	FirstName
9	Job Title	JobTitle
10	Language	Language
11	Last Name	LastName
12	Legal Entity	CustomText2
13	Middle Name	MiddleName
14	Password	__PASSWORD__
15	Region	Region
16	Reports To	ManagerFullName
17	Return Id	__UID__
18	RohanField	CustomText2
19	Role[LOOKUP]	Role
20	User Login Id	UserLoginId
21	Work Phone	PhoneNumber

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 [Creating a New UI Form](#) and [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.

 **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 [Setting up the Lookup Definition for User Operations](#) for more information.

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.crmmod.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 (#):

```
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:
`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.crmmod.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:

 **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:

Upload JARs Utility in *Oracle Fusion Middleware Developing and Customizing Applications 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.

Note:

The Lookup.CRMOD.UM.ReconTransformations lookup definition is optional and does not exist by default.

You must add this lookup as decode value to the Lookup.CRMOD.UM.Configuration lookup definition to enable exclusions during provisioning and reconciliation operations. See [Setting up the Lookup Definition for User Operations](#) for more information.

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:

```
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.
3. Create a new lookup definition, **Lookup.CRMOD.UM.ReconTransformations**.
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.crmmod.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:**

Upload JARs Utility in *Oracle Fusion Middleware Developing and Customizing Applications 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.

 **Note:**

The Lookup.CRMOD.UM.ProvExclusionList and Lookup.CRMOD.UM.ReconExclusionList 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 [Setting up the Lookup Definition for User Operations](#) for more information.

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

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

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:

Code Key	Decode
User Login Id	User001
User Login Id	User002
User Login Id	User088

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>

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:

Code Key	Decode
User Login Id[PATTERN]	User001 User002 User088

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:

Code Key	Decode
User Login Id[PATTERN]	00012*

6. Click the save icon.

5

Known Issues

This 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.