

Oracle® Identity Manager

Connector Guide for BMC Remedy User Management

Release 9.0.4

E10422-05

August 2009

Oracle Identity Manager Connector Guide for BMC Remedy User Management, Release 9.0.4

E10422-05

Copyright © 2009, Oracle and/or its affiliates. All rights reserved.

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, 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 software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software 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 which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on 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. 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.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vi
Conventions	vi
What's New in the Oracle Identity Manager Connector for BMC Remedy User Management?	vii
Software Updates	vii
Documentation-Specific Updates.....	viii
1 About the Connector	
1.1 Connector Architecture	1-1
1.2 Reconciliation Module	1-2
1.2.1 Lookup Fields Reconciliation.....	1-2
1.2.2 User Reconciliation.....	1-3
1.2.2.1 Reconciled Resource Object Fields.....	1-3
1.2.2.2 Reconciled Xellerate User Fields	1-4
1.3 Provisioning Module	1-4
1.4 Supported Functionality	1-5
1.5 Multilanguage Support	1-6
1.6 Files and Directories That Comprise the Connector	1-6
1.7 Determining the Release Number of the Connector.....	1-7
2 Deploying the Connector	
2.1 Verifying Deployment Requirements.....	2-1
2.2 Copying the External Code Files	2-2
2.2.1 Oracle Identity Manager Running on Microsoft Windows.....	2-2
2.2.2 Oracle Identity Manager Running on Linux or Solaris.....	2-2
2.3 Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later.....	2-3
2.3.1 Running the Connector Installer	2-3
2.3.2 Configuring the IT Resource	2-5
2.4 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.1	2-6
2.4.1 Copying the Connector Files.....	2-6

2.4.2	Importing the Connector XML File.....	2-7
2.5	Configuring the Target System.....	2-9
2.5.1	Enabling Encryption.....	2-9
2.5.1.1	Configuring Remedy Encryption.....	2-9
2.5.1.2	AR System Encryption Error Messages	2-10
2.6	Configuring the Oracle Identity Manager Server	2-11
2.6.1	Changing to the Required Input Locale	2-11
2.6.2	Clearing Content Related to Connector Resource Bundles from the Server Cache	2-11
2.6.3	Enabling Logging.....	2-12

3 Configuring the Connector

3.1	Configuring Reconciliation.....	3-1
3.1.1	Partial Reconciliation.....	3-1
3.1.2	Batched Reconciliation.....	3-2
3.1.3	Configuring Trusted Source Reconciliation.....	3-3
3.1.4	Configuring the Reconciliation Scheduled Tasks	3-3
3.1.4.1	Specifying Values for the Scheduled Task Attributes.....	3-4
3.1.4.1.1	Lookup Fields Reconciliation Scheduled Task	3-4
3.1.4.1.2	User Reconciliation Scheduled Tasks.....	3-6
3.1.5	Adding Custom Attributes for Reconciliation	3-8
3.2	Configuring Provisioning.....	3-10
3.2.1	Compiling Adapters.....	3-10
3.2.2	Adding Custom Attributes for Provisioning.....	3-11
3.3	Configuring the Connector for Multiple Installations of the Target System	3-14

4 Testing and Troubleshooting

4.1	Testing the Connector	4-1
4.1.1	Testing Partial and Batched Reconciliation	4-1
4.2	Troubleshooting Connector Problems.....	4-2

5 Known Issues

A Attribute Mappings Between Oracle Identity Manager and BMC Remedy User Management

Index

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with BMC Remedy User Management.

Audience

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

Documentation Accessibility

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

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

Deaf/Hard of Hearing Access to Oracle Support Services

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

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

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

<http://www.oracle.com/technology/documentation/oim.html>

Documentation Updates

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

<http://www.oracle.com/technology/documentation/oim.html>

Conventions

The following text conventions are used in this document:

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

What's New in the Oracle Identity Manager Connector for BMC Remedy User Management?

This chapter provides an overview of the updates made to the software and documentation for the BMC Remedy User Management connector in release 9.0.4.2 of the connector.

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

- [Software Updates](#)
These include updates made to the connector software.
- [Documentation-Specific Updates](#)
These include major changes made to the connector documentation. These changes are not related to software updates.

Software Updates

The following sections discuss the software updates:

- [Software Updates in Releases 9.0.4 and 9.0.4.1](#)
- [Software Updates in Release 9.0.4.2](#)

Software Updates in Releases 9.0.4 and 9.0.4.1

The following are software updates in releases 9.0.4 and 9.0.4.1:

- [Changes in the Directory Structure for the Connector Installation Files](#)

Changes in the Directory Structure for the Connector Installation Files

In this release of the connector, the `BMCTrigger` directory has been changed to the `scripts` directory. Corresponding changes have been made in various sections in this guide.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- [Support for the Connector Installer](#)
- [Support for BMC Remedy AR System 7.1](#)
- [Extended Multilanguage Support](#)

- [Additions to the Known Issues List](#)
- [Resolved Issues in Release 9.0.4.2](#)

Support for the Connector Installer

From Oracle Identity Manager release 9.1.0 onward, the Administrative and User Console provides the Connector Installer feature. This feature can be used to automate the connector installation procedure.

See "[Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later](#)" for more information.

Support for BMC Remedy AR System 7.1

From this release onward, the connector supports BMC Remedy AR System 7.1. Changes related to this software update have been made in various sections in this guide.

Note: BMC Remedy AR System 6.0 is unsupported from this release onward.

Extended Multilanguage Support

From this release onward, the connector supports the 12 languages listed in the "[Multilanguage Support](#)" section.

Some of the entries in the resource bundles have not been translated. See the "[Known Issues](#)" chapter for more information.

Additions to the Known Issues List

The issue tracked by Bug 8367021 has been added in the "[Known Issues](#)" chapter.

Resolved Issues in Release 9.0.4.2

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
7646231	The connector could be used only on an Oracle Identity Manager installation running on Microsoft Windows.	This issue has been resolved. The connector can now be used on Oracle Identity Manager installations running on Microsoft Windows, Linux, and Solaris. See " Copying the External Code Files " for information about the required code files on each of the supported operating systems.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- The limitation that the target system does not support SSL communication has been moved from the "[Known Issues](#)" chapter to the "[Verifying Deployment Requirements](#)" section.
- In the "[Verifying Deployment Requirements](#)" section, changes have been made in the "Target Systems" row.
- The location for copying the arapi70.jar and arutil70.jar files has been modified in the following sections:

- Oracle Identity Manager Running on Microsoft Windows
- Oracle Identity Manager Running on Linux or Solaris

About the Connector

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

This chapter contains the following sections:

- [Connector Architecture](#)
- [Reconciliation Module](#)
- [Provisioning Module](#)
- [Supported Functionality](#)
- [Multilanguage Support](#)
- [Files and Directories That Comprise the Connector](#)
- [Determining the Release Number of the Connector](#)

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

At some places in this guide, BMC Remedy System has been referred to as the *target system*. It is used interchangeably with BMC Remedy User Management.

The BMC Remedy User Management connector is also referred to as the user management connector.

1.1 Connector Architecture

The architecture of the connector is the blueprint for the functionality of the connector.

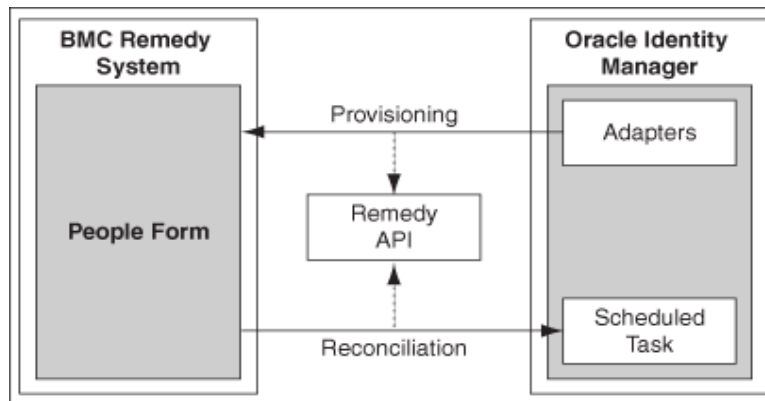
The primary function of a connector is to create Users on the target system through Oracle Identity Manager. The BMC Remedy System (target system) can be configured to run in either the identity reconciliation (trusted source) mode or the provisioning (target resource) mode.

In the identity reconciliation mode, BMC Remedy System is used as the trusted source and users are directly created and modified on it. During reconciliation from the trusted source, the user management connector fetches data about these target system users into Oracle Identity Manager. This data is used to create or update the corresponding OIM Users.

In the account management or provisioning mode, BMC Remedy System is used as a target resource. During reconciliation, the user management connector fetches data about users created or modified directly on the target system into Oracle Identity Manager. This data is used to add or modify resources allocated to OIM Users. In addition, the connector enables provisioning operations through which user data changes are propagated from Oracle Identity Manager to BMC Remedy System.

Figure 1–1 provides the architecture of the BMC Remedy User Management connector.

Figure 1–1 Architecture of the BMC Remedy User Management Connector



Users are created during provisioning in the People form of the BMC Remedy target system. The connector makes use of the Remedy APIs to connect to the Remedy Server, and in turn provision the account.

During Reconciliation, user records are retrieved from the People form.

1.2 Reconciliation Module

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

See Also: The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about reconciliation configurations

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

- [Lookup Fields Reconciliation](#)
- [User Reconciliation](#)

1.2.1 Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the following lookup fields:

- Company
- Organization
- Department
- Region

- Site
- Site ID
- Site Group
- Support Group ID
- Support Relationship Role
- Support Group Company
- Support Group Organization
- Support Group Name
- Primary Cost Center Code

1.2.2 User Reconciliation

User reconciliation involves reconciling the following fields.

1.2.2.1 Reconciled Resource Object Fields

The following target system fields are reconciled:

- Profile Status
- ARLicenseType
- Department
- Site
- Region
- LastName
- FirstName
- LoginName
- SupportStaff
- HourlyRate
- Vip
- Client Type
- Client Sensitivity
- NotificationMethod
- EmailAddress
- PrimaryCenterCode
- Company
- Organization
- Site ID
- Person ID
- Business Phone Number

The following multivalued fields are reconciled:

- Support Group Company

- Support Group Organization
- Support Group Name
- Support Group Relationship Role
- Support Group Association ID
- Support Group ID

1.2.2.2 Reconciled Xellerate User Fields

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

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

1.3 Provisioning Module

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

See Also: The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Concepts Guide* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- Profile Status
- ARLicenseType
- Department
- Site
- Region
- LastName
- FirstName
- LoginName
- HourlyRate
- Vip
- Client Type
- Client Sensitivity
- NotificationMethod
- EmailAddress
- PrimaryCenterCode

- Password
- Company
- Organization
- Site Group

The following multivalued fields are provisioned:

- Support Group Company
- Support Group Organization
- Support Group Name
- Support Group Relationship Role
- Support Group ID

Note: If a support group is added, then the SupportStaff field on the parent form is updated to Yes.

1.4 Supported Functionality

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

Function	Type	Description
Add User	Provisioning	Creates a user
Delete User	Provisioning	Deletes a user
Update User Last Name	Provisioning	Updates the last name of a user
Update User Password	Provisioning	Updates the password of a user
Update User First Name	Provisioning	Updates the first name of a user
Update User Client Sensitivity	Provisioning	Updates the Client Sensitivity field of a user
Update User Email	Provisioning	Updates the e-mail address of a user
Update User Support Staff	Provisioning	Updates the support staff of a user
Update User Profile Status	Provisioning	Updates the profile status of a user
Update User Client Type	Provisioning	Updates the client type of a user
Update User VIP Field	Provisioning	Updates the VIP status of a user
Update User Business Phone	Provisioning	Updates the business phone number of a user
Update User Notification Method Field	Provisioning	Updates the notification method of a user
Update User Region	Provisioning	Updates the region of a user
Update User Site	Provisioning	Updates the site of a user
Update User Department	Provisioning	Updates the department of a user
Update User Company	Provisioning	Updates the company of a user
Update User Organization	Provisioning	Updates the organization of a user
Update User Hourly Rate	Provisioning	Updates the hourly rate of a user

Function	Type	Description
Update User CostCentercode	Provisioning	Updates the cost center code of a user
Update User ARLicenseType	Provisioning	Updates the ARLicense type of a user
Update User Site Group	Provisioning	Updates the User Site group of a user
Reconcile Lookup Field	Reconciliation	Reconciles the lookup fields
Reconcile User Data	Reconciliation	Trusted source reconciliation: Reconciles user data from BMC Remedy User Management to Oracle Identity Manager. A corresponding user is created in Oracle Identity Manager. If the user already exists in Oracle Identity Manager, then this user is updated. Target resource reconciliation: Reconciles user data from BMC Remedy User Management to Oracle Identity Manager. A user is not created in Oracle Identity Manager.

See Also: [Appendix A, "Attribute Mappings Between Oracle Identity Manager and BMC Remedy User Management"](#)

1.5 Multilanguage Support

The connector supports the following languages:

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

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

1.6 Files and Directories That Comprise the Connector

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

Help Desk/BMC Remedy/BMC Remedy User Management

These files and directories are listed in [Table 1-1](#).

Table 1–1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
configuration/BMC RemedyUser Reconciliation-CI.xml	This XML file contains configuration information that is used during connector installation.
config/attributemapping_prov.properties	This file contains the attributes required for provisioning.
config/attributemapping_recon.properties	This file contains the attributes required for reconciliation.
lib/JavaTask/xlBMCRemedy.jar	This file contains the class files that are required for provisioning.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. Note: A resource bundle is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
test/config/config.properties	This file contains the parameters required to connect to and perform provisioning on the target system.
test/config/log.properties	This file is used to store log information.
test/scripts/BMCRemedy.bat test/scripts/BMCRemedy.sh	This file is used to run the test utility.
xml/BMCConnector_DM.xml	This file contains definitions for the following components of the connector: <ul style="list-style-type: none"> ■ IT resource type ■ IT resource ■ Resource object ■ Process form ■ Process definition ■ Process tasks ■ Adapter tasks ■ Scheduled tasks
xml/BMCXellerateUser_DM.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector for trusted source reconciliation.

1.7 Determining the Release Number of the Connector

You can use the following method to determine the release number of the connector:

1. Extract the contents of the `xlBMCRemedy.jar` file. This file is in the following directory on the installation media:

```
OIM_HOME/xellerate/JavaTasks/xlBMCRemedy.jar
```

2. Open the `Manifest.mf` file in a text editor. The `Manifest.mf` file is one of the files bundled inside the `xlBMCRemedy.jar` file.

In the `Manifest.mf` file, the release number of the connector is displayed as the value of the `Version` property.

Deploying the Connector

Deploying the connector involves the following steps:

- [Verifying Deployment Requirements](#)
- [Copying the External Code Files](#)
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
 - [Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later](#)
 - [Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.1](#)
- [Configuring the Target System](#)
- [Configuring the Oracle Identity Manager Server](#)

2.1 Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target systems	BMC Remedy AR System 7.x Note: The target system does not support SSL communication.
External code files	The set of required files depends on the operating system on which Oracle Identity Manager is running. See " Copying the Connector Files " for more information.
Target system user account	User account that is a member of the APP-Administrator group You provide the credentials of this user account while defining the IT resource. The procedure is described later in this guide. If the specified privileges were not assigned to the target system user account, then the following message would be displayed: <code>You do not have write access.</code>

2.2 Copying the External Code Files

Depending on the operating system on which Oracle Identity Manager is running, perform the procedure described in one of the following sections:

Note: While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the contents of the `connectorResources` directory and the JAR files to the corresponding directories on each node of the cluster.

- [Oracle Identity Manager Running on Microsoft Windows](#)
- [Oracle Identity Manager Running on Linux or Solaris](#)

2.2.1 Oracle Identity Manager Running on Microsoft Windows

To copy external code files on Oracle Identity Manager running on Microsoft Windows:

1. Copy the `arapi70.jar` and `arutil70.jar` files from the BMC Remedy Admin Client installation directory (for example, `C:\Program Files\AR System`) to the `JAVA_HOME/jre/lib/ext` directory. Here, `JAVA_HOME` is the location of the JDK directory for your application server.
2. Copy the following files from the BMC Remedy Admin Client installation directory to the `OIM_HOME/xellerate/ThirdParty` directory:

Note: If you do not have these files in your target system installation directory, then check with your vendor.

```
arapi70.dll
arjni70.dll
arrpc70.dll
arutil70.dll
icudt32.dll
icuin32.dll
icuuc32.dll
```

3. Include `OIM_HOME/xellerate/ThirdParty` in the `PATH` environment variable.

2.2.2 Oracle Identity Manager Running on Linux or Solaris

To copy external code files on Oracle Identity Manager running on Linux or Solaris:

1. Copy the `arapi70.jar` and `arutil70.jar` files from the BMC Remedy Admin Client installation directory (for example, `BMC_HOME/ar/mid-tier/WEB-INF/lib/`) to the `JAVA_HOME/jre/lib/ext` directory. Here, `JAVA_HOME` is the location of the JDK directory for your application server.
2. Copy the following files from the BMC Remedy Admin Client installation directory to the `OIM_HOME/xellerate/ThirdParty` directory:

Note: If you do not have these files in your target system installation directory, then check with your vendor.

These .so files are different for different (for example, x86 and SPARC) platforms. Ensure that you use the .so files that are specific to the type of platform on which Oracle Identity Manager is running.

libarjni70.so
 libarutiljni70.so
 libicudatabmc.so
 libicudatabmc.so.32
 libicui18nbmc.so
 libicui18nbmc.so.32
 libicuiobmc.so
 libicuiobmc.so.32
 libicuucbmc.so
 libicuucbmc.so.32

3. Add the following lines at the end of the system profile file:

```
LD_LIBRARY_PATH=OIM_HOME/xellerate/ThirdParty
export LD_LIBRARY_PATH
```

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

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

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

- [Running the Connector Installer](#)
- [Configuring the IT Resource](#)

2.3.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media into the following directory:
OIM_HOME/xellerate/ConnectorDefaultDirectory
2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of *Oracle Identity Manager Administrative and User Console*.
3. Click **Deployment Management**, and then click **Install Connector**.

4. From the Connector List list, select **BMC Remedy User Management** *RELEASE_NUMBER*. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory:

OIM_HOME/xellerate/ConnectorDefaultDirectory

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

- a. In the **Alternative Directory** field, enter the full path and name of that directory.
 - b. To repopulate the list of connectors in the Connector List list, click **Refresh**.
 - c. From the Connector List list, select **BMC Remedy User Management** *RELEASE_NUMBER*.
5. Click **Load**.
 6. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

- a. Configuration of connector libraries
- b. Import of the connector XML files (by using the Deployment Manager)
- c. Compilation of adapters

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

- Retry the installation by clicking **Retry**.
 - Cancel the installation and begin again from Step 1.
7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:
 - a. Ensuring that the prerequisites for using the connector are addressed

Note: At this stage, run the `PurgeCache` utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. Refer to "[Clearing Content Related to Connector Resource Bundles from the Server Cache](#)" on page 2-11 for information about running the `PurgeCache` utility.

There are no prerequisites for some predefined connectors.

- b. Configuring the IT resource for the connector
Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.
- c. Configuring the scheduled tasks that are created when you installed the connector
Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

You must manually copy the following files to the specified destination directories:

File in the Installation Media Directory	Destination Directory
Files in the <code>config</code> directory	<code>OIM_HOME/xellerate/XLIntegrations/BMC/config</code>
Files in the <code>test/config</code> directory	
Files in the <code>test/scripts</code> directory	<code>OIM_HOME/xellerate/XLIntegrations/BMC/scripts</code>

Installing the Connector in an Oracle Identity Manager Cluster

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

2.3.2 Configuring the IT Resource

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

You must specify values for the parameters of the BMC IT resource as follows:

1. Log in to the Administrative and User Console.
2. Expand **Resource Management**.
3. Click **Manage IT Resource**.
4. In the IT Resource Name field on the Manage IT Resource page, enter **BMC** and then click **Search**.
5. Click the edit icon for the IT resource.
6. From the list at the top of the page, select **Details and Parameters**.
7. Specify values for the parameters of the IT resource. The following table describes each parameter:

Parameter	Description
<code>UserName</code>	User ID that is used to connect to the target system The default value is <code>Demo</code> .
<code>Password</code>	Password for the user ID that is used to connect to the target system
<code>ServerName</code>	IP address or computer name of the BMC Remedy User Management server
<code>Port</code>	TCP/IP port at which the BMC Remedy User Management server is listening The default value is <code>0</code> .
<code>TrustedField</code>	Unique identification key for searching user records The default value is <code>Person ID</code> .
<code>TrustedTimeStamp</code>	This parameter is used for trusted source reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is <code>None</code> . Do not change it.

Parameter	Description
NonTrustedTimeSt amp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is None . Do not change it.
IsSecure	Specifies whether or not the encryption feature is enabled The value can be YES or NO . The default value is NO .
DeleteUserFormNa me	Name of the form in the target system from which details of deleted users can be obtained The value is CTM: People .
FormName	Name of the form in the target system from which details of newly created and updated users can be obtained The value is CTM: People .
NumberOfTrials	Number of times the connection to the target system must be retried before the InvocationTargetException is thrown Default value: 2
DelayBetweenTria ls	Time difference between subsequent retries (in milliseconds) Default value: 20000
SupportGroupForm Name	Name of the form on the target system from which details of newly created and updated support group for a user can be obtained The value is CTM: Support Group Association .
SupportGroupTrus tedField	Unique identification key for searching support group records for a user. The default value is Support Group Association ID.

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

2.4 Installing the Connector on Oracle Identity Manager Release 8.5.3.1 Through 9.0.3.1

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

- [Copying the Connector Files](#)
- [Importing the Connector XML File](#)

2.4.1 Copying the Connector Files

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

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following directory on the installation media:

Help Desk/BMC Remedy/BMC Remedy User Management

Refer to the ["Files and Directories That Comprise the Connector"](#) section for more information about these files.

File in the Installation Media Directory	Destination Directory
Files in the <code>config</code> directory	<code>OIM_HOME/xellerate/XLIntegrations/BMC/config</code>
Files in the <code>test/config</code> directory	
<code>lib/JavaTask/xlBMCRemedy.jar</code>	<code>OIM_HOME/xellerate/JavaTasks</code>
File in the <code>resources</code> directory	<code>OIM_HOME/xellerate/connectorResources</code>
Files in the <code>test/scripts</code> directory	<code>OIM_HOME/xellerate/XLIntegrations/BMC/scripts</code>
<code>xml/BMCConnector_DM.xml</code>	<code>OIM_HOME/xlclient</code>
<code>xml/BMCXellerateUser_DM.xml</code>	

2.4.2 Importing the Connector XML File

As mentioned in the ["Files and Directories That Comprise the Connector"](#) section, the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML file into Oracle Identity Manager:

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

Parameter	Description
<code>UserName</code>	User ID that is used to connect to the target system The default value is <code>Demo</code> .
<code>Password</code>	Password for the user ID that is used to connect to the target system

Parameter	Description
ServerName	IP address or computer name of the BMC Remedy User Management server
Port	TCP/IP port at which the BMC Remedy User Management server is listening The default value is 0.
TrustedField	Unique identification key for searching user records The default value is Person ID.
TrustedTimeStamp	This parameter is used for trusted source reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is None. Do not change it.
NonTrustedTimeStamp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is None. Do not change it.
IsSecure	Specifies whether or not the encryption feature is enabled The value can be YES or NO. The default value is NO.
DeleteUserFormName	Name of the form in the target system from which details of deleted users can be obtained The value is CTM:Delete.
FormName	Name of the form in the target system from which details of newly created and updated users can be obtained The value is CTM:People.
NumberOfTrials	Number of times the connection to the target system must be retried before the InvocationTargetException is thrown Default value: 2
DelayBetweenTrials	Time difference between subsequent retries (in milliseconds) Default value: 20000
SupportGroupFormName	Name of the form on the target system from which details of newly created and updated support group for a user can be obtained The default value is CTM:Support Group Association.
SupportGroupTrustedField	Unique identification key for searching support group records for a user. The default value is Support Group Association ID.

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

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

11. Click **View Selections**.

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

12. Click **Import**. The connector XML file is imported into Oracle Identity Manager. After you import the connector XML file, proceed to the next chapter.

2.5 Configuring the Target System

Configuring the target system involves the following steps:

- [Enabling Encryption](#)

2.5.1 Enabling Encryption

This section discusses the following topics related to Remedy encryption:

- [Configuring Remedy Encryption](#)
- [AR System Encryption Error Messages](#)

2.5.1.1 Configuring Remedy Encryption

To enable encryption and set encryption options, you must include server encryption options in the `ar.conf` file (UNIX) or the `ar.cfg` file (Microsoft Windows). You can do this by using a text editor.

You can set the `Encrypt-Security-Policy` encryption option. This is an integer value that indicates whether or not encryption is enabled. If this option is not in the `ar.cfg` (or `ar.conf`) file, then encryption is disabled by default. If encryption is enabled, then you can set encryption to any one of the following values to this option:

- **0:** Encryption is allowed. Clients and servers with or without encryption enabled on them can connect to this AR System server.
- **1:** Encryption is required. Only clients and servers that have encryption enabled on them can connect to this AR System server.
- **2:** Encryption is disallowed. Regardless of whether or not encryption is enabled, clients and servers can communicate without encryption.

The following table explains sample settings for the options that you can add in the `ar.conf` (or `ar.cfg`) file.

Option Settings	Significance
<code>Encrypt-Security-Policy: 1</code>	Encryption is required.
<code>Encrypt-Public-Key-Expire: 86400</code>	Public key duration is 1 day (86400 seconds).
<code>Encrypt-Symmetric-Data-Key-Expire: 2700</code>	Symmetric data encryption key duration is 45 minutes (2700 seconds).
<code>Encrypt-Public-Key-Algorithm: 5</code>	Public key encryption key strength is RSA-1024 (Performance Security).
<code>Encrypt-Data-Encryption-Algorithm: 2</code>	Symmetric data encryption key strength is RC4 128-bit (Performance Security).

If you do not set these options, then the default values are used. Defaults for the level of encryption depend on the encryption product that you are using.

To enable Remedy encryption:

1. Exit or stop all AR System processes that are running.

To do this, open **Control Panel**, **Administrator Tools**, and **Services**. Stop each AR System process that is running.

2. In the `ar.conf` file (for UNIX) or the `ar.cfg` file (for Microsoft Windows), add the `Encrypt-Security-Policy` option with a setting of 0 (encryption is allowed) or 1 (encryption is required). Add other options in the file as required.

The default UNIX directory for the `ar.conf` file is `ar_install_dir/conf`. In Microsoft Windows, the `ar.cfg` file is stored in the `ar_install_dir\conf` directory. Here, `ar_install_dir` is the installation directory for ARSystem on the AR server.

Caution: If you set the `Encrypt-Security-Policy` option to 1 (encryption is required), then communication is not allowed for any server or client that has not been upgraded to use encryption.

3. Restart the AR System server.

2.5.1.2 AR System Encryption Error Messages

When the AR System server is started, it checks encryption licensing and encryption configuration settings, if encryption is enabled. If the appropriate Remedy Encryption product licenses are not detected or if invalid configuration settings are detected, then one or more of the following error messages are displayed.

Error Number	Error Message and Description
9010	Encryption is enabled, but the encryption library is not found. Install the Remedy Encryption product.
9012	No encryption license. Add the encryption license for the Remedy Encryption product that you are using.
9013	The encryption license does not match the type of Remedy Encryption product that is installed. Obtain the license for the type of Remedy Encryption product that is installed.
9006	The encryption library does not support the specified public key encryption algorithm. Set the <code>Encryption-Public-Key-Algorithm</code> option in the <code>ar.cfg</code> (or <code>ar.conf</code>) file to a value that is supported by the type of AR System Encryption product that is installed.
9007	The encryption library does not support the specified data encryption algorithm. Set the <code>Encrypt-Data-Encryption-Algorithm</code> option in the <code>ar.cfg</code> (or <code>ar.conf</code>) file to a value that is supported by the type of AR System Encryption product that is installed.

If encryption is disabled, then encryption error checking does not occur and encryption errors are bypassed. Error messages are listed in the order in which they are detected.

2.6 Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

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

- [Changing to the Required Input Locale](#)
- [Clearing Content Related to Connector Resource Bundles from the Server Cache](#)
- [Enabling Logging](#)

2.6.1 Changing to the Required Input Locale

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

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

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

When you perform the deployment procedure, files from the resources directory on the installation media are copied into the `OIM_HOME/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

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

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

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

2. Enter one of the following commands:

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

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

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

`OIM_HOME/xellerate/config/xlConfig.xml`

2.6.3 Enabling Logging

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

- ALL
This level enables logging for all events.
- DEBUG
This level enables logging of information about fine-grained events that are useful for debugging.
- INFO
This level enables logging of messages that highlight the progress of the application at a coarse-grained level.
- WARN
This level enables logging of information about potentially harmful situations.
- ERROR
This level enables logging of information about error events that may allow the application to continue running.
- FATAL
This level enables logging of information about very severe error events that could cause the application to stop functioning.
- OFF
This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **BEA WebLogic Server**

To enable logging:

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

```
log4j.logger.Adapter.BMCRemedy=log_level
```
2. In this line, replace `log_level` with the log level that you want to set.

For example:

```
log4j.logger.Adapter.BMCRemedy=INFO
```

After you enable logging, log information is written to the following file:

`WebLogic_home/user_projects/domains/domain_name/server_name/server_name.log`

- **IBM WebSphere Application Server**

To enable logging:

1. Add the following line in the

OIM_HOME/xellerate/config/log.properties file:

```
log4j.logger.Adapter.BMCRemedy=log_level
```

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

For example:

```
log4j.logger.Adapter.BMCRemedy=INFO
```

After you enable logging, log information is written to the following file:

WebSphere_home/AppServer/logs/server_name/startServer.log

- **JBoss Application Server**

To enable logging:

1. In the *JBoss_home/server/default/conf/log4j.xml* file, locate the following lines:

```
<category name="Adapter.BMCRemedy">
  <priority value="log_level"/>
</category>
```

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

```
<category name="Adapter.BMCRemedy">
  <priority value="INFO"/>
</category>
```

After you enable logging, log information is written to the following file:

JBoss_home/server/default/log/server.log

- **Oracle Application Server**

To enable logging:

1. Add the following line in the

OIM_HOME/xellerate/config/log.properties file:

```
log4j.logger.Adapter.BMCRemedy=log_level
```

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

For example:

```
log4j.logger.Adapter.BMCRemedy=INFO
```

After you enable logging, log information is written to the following file:

OC4J_home/opmn/logs/default_group~home~default_group~1.log

Configuring the Connector

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

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

- [Configuring Reconciliation](#)
- [Configuring Provisioning](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)

3.1 Configuring Reconciliation

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

- [Configuring Trusted Source Reconciliation](#)
- [Partial Reconciliation](#)
- [Batched Reconciliation](#)
- [Configuring the Reconciliation Scheduled Tasks](#)
- [Adding Custom Attributes for Reconciliation](#)

3.1.1 Partial Reconciliation

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

Creating a filter involves specifying a value for a target system attribute, which will be used in the query SELECT criteria to retrieve the records to be reconciled. You can specify values for any one or a combination of the following target system attributes:

- First Name

- Last Name
- Status
- Notification Method

If you want to use multiple target system attributes to filter records, then you must also specify the logical operator (AND or OR) that you want to apply to the combination of target system attributes that you select.

For example, suppose you specify the following values for these attributes:

- First Name: John
- Last Name: Doe
- Status: 1
- Notification Method: 1
- Operator: OR

Because you are using the OR operator, during reconciliation, only user records for which *any one* of these criteria is met are reconciled. If you were to use the AND operator, then only user records for which *all* of these criteria are met are reconciled.

While deploying the connector, follow the instructions in the "[Specifying Values for the Scheduled Task Attributes](#)" section on page 3-4 to specify values for these attributes and the logical operator that you want to apply.

3.1.2 Batched Reconciliation

During a reconciliation run, all changes in the target system records are reconciled into Oracle Identity Manager. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid these problems.

To configure batched reconciliation, you must specify values for the following user reconciliation scheduled task attributes:

- `BatchSize`: Use this attribute to specify the number of records that must be included in each batch. The default value is 1000.
- `NumberOfBatches`: Use this attribute to specify the total number of batches that must be reconciled. The default value is `All`.

If you specify a value other than `All`, then some of the newly added or modified user records may not get reconciled during the current reconciliation run. The following example illustrates this:

Suppose you specify the following values while configuring the scheduled tasks:

- `BatchSize`: 20
- `NumberOfBatches`: 10

Suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 200 records would be reconciled during the current reconciliation run. The remaining 114 records would be reconciled during the next reconciliation run.

You specify values for the `BatchSize` and `NumberOfBatches` attributes by following the instructions described in the "[Specifying Values for the Scheduled Task Attributes](#)" section on page 3-4.

3.1.3 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or a target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

Note: You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

Note: You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

1. Import the XML file for trusted source reconciliation, `BMCXellerateUser_DM.xml`, by using the Deployment Manager. This section describes the procedure to import the XML file.

Note: Only one target system can be designated as a trusted source. If you import the `BMCXellerateUser_DM.xml` file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Specify values for the attributes of the `BMC Trusted User Reconciliation` scheduled task. This procedure is described later in this guide.

To configure trusted source reconciliation:

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

3.1.4 Configuring the Reconciliation Scheduled Tasks

When you perform the deployment procedure, the scheduled tasks for lookup fields, trusted source user, and target resource user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

1. Open the Oracle Identity Manager Design Console.

2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler**.
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. Oracle Identity Manager must attempt to complete the task before assigning the **FAILED** status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
 - To set the task to run on a recurring basis, select the **Daily, Weekly, Recurring Intervals, Monthly, or Yearly** option.
If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
 - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "[Specifying Values for the Scheduled Task Attributes](#)" section on page 3-4 for information about the values to be specified.

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

After you configure all three scheduled tasks, proceed to the "[Adding Custom Attributes for Reconciliation](#)" section on page 3-8.

3.1.4.1 Specifying Values for the Scheduled Task Attributes

Refer to the following sections for information about the attribute values to be specified for the scheduled tasks:

- [Lookup Fields Reconciliation Scheduled Task](#)
This section describes attributes of the lookup fields reconciliation scheduled task.
- [User Reconciliation Scheduled Tasks](#)
This section describes attributes of the user reconciliation scheduled tasks for both trusted source and target resource.

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

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Value
ServerName	Name of the IT resource	BMC
TargetRO	Name of the resource object	BMCRO
LookUpCodeKey	Name of the lookup code	The value can be any one of the following: <ul style="list-style-type: none"> ■ Region ■ Site ■ Department ■ Company ■ Organization ■ SiteGroup ■ SiteID ■ SupportGroupCompany ■ SupportGroupOrganization ■ SupportGroupName ■ RelationshipRole ■ SupportGroupID ■ PrimaryCenterCode
LookUpFieldCode	Name of the lookup field	You must enter the value corresponding to the LookUpCodeKey value that you specify: <ul style="list-style-type: none"> ■ Lookup.BMC.Region ■ Lookup.BMC.Site ■ Lookup.BMC.Department ■ Lookup.BMC.Company ■ Lookup.BMC.Organization ■ Lookup.BMC.SiteGroup ■ Lookup.BMC.SiteID ■ Lookup.BMC.SupportCompany ■ Lookup.BMC.SupportOrganization ■ Lookup.BMC.SupportGroup ■ Lookup.BMC.RelationshipRole ■ Lookup.BMC.SupportGroupID ■ Lookup.BMC.PrimaryCentercode <p>For example, if you enter SupportGroupID as the LookUpCodeKey value, then you must enter Lookup.BMC.SupportGroupID as the LookUpFieldCode value.</p>

Attribute	Description	Value
LookupFormName	Form name to retrieve lookup values	<p>You must enter the value corresponding to the LookUpCodeKey value that you specify:</p> <ul style="list-style-type: none"> ■ SIT:Site Group ■ SIT:Site Alias Company LookUp ■ CTM:People Organization ■ CTM:People Organization ■ CTM:People Organization ■ CTM:Region ■ SIT:Site ■ CTM:Support Group ■ CTM:Support Group ■ CTM:Support Group ■ SYS:Menu Items ■ CTM:Support Group ■ FIN:ConfigCostCentersRepository <p>For example, if you enter SupportGroupID as the LookUpCodeKey value, then you must enter CTM:Support Group as the LookupFormName value.</p>

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

3.1.4.1.2 User Reconciliation Scheduled Tasks Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled tasks:

- BMC Trusted User Reconciliation (Scheduled task for trusted source reconciliation)
- BMC Non Trusted User Reconciliation (Scheduled task for target resource reconciliation)

The following table describes the attributes of both scheduled tasks.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Attribute	Description	Value
ServerName	Name of the IT resource	BMC

Attribute	Description	Value
IsTrusted	Specifies whether or not reconciliation is to be carried out in trusted mode	For trusted source reconciliation, set the value of this attribute to <code>Yes</code> . For target resource reconciliation, set the value of this attribute to <code>No</code> .
TargetRO	Name of the resource object	BMCRO
XellerateOrganization	Default value for the Oracle Identity Manager Organization name This value is used to create the Xellerate User in trusted mode. Note: This attribute is specific to the scheduled task for trusted source reconciliation.	Xellerate Users
BatchSize	Number of records in each batch that is reconciled You must specify an integer value greater than zero. See Also: The " Batched Reconciliation " section on page 3-2	The default value is 1000.
NoOfBatches	Number of batches to be reconciled The number of records in each batch is specified by the <code>BatchSize</code> attribute. See Also: The " Batched Reconciliation " section on page 3-2	Specify <code>All</code> if you want to reconcile all the batches. This is the default value. Specify an integer value greater than zero if you want to reconcile only a fixed number of batches.
First Name	This is a filter attribute. Use this attribute to specify the first name of the user whose records you want to reconcile. If you do not want to use this filter attribute, then specify <code>Nodata</code> . See Also: The " Partial Reconciliation " section on page 3-1	The value can be either the first name or <code>Nodata</code> . The default value is <code>Nodata</code> .
Last Name	This is a filter attribute. Use this attribute to specify the last name of the user whose records you want to reconcile. If you do not want to use this filter attribute, then specify <code>Nodata</code> . See Also: The " Partial Reconciliation " section on page 3-1	The value can be either the last name or <code>Nodata</code> . The default value is <code>Nodata</code> .
Notification Method	This is a filter attribute. Use this attribute to specify the notification method for which you want to reconcile user records. If you do not want to use this filter attribute, then specify <code>Nodata</code> . See Also: The " Partial Reconciliation " section on page 3-1	The value can be either the notification method or <code>Nodata</code> . The default value is <code>Nodata</code> . The notification method value can be one of the following numbers: <ul style="list-style-type: none"> ■ 0 (None) ■ 1 (Alert) ■ 2 (Email) ■ 3 (User Default)

Attribute	Description	Value
Status	<p>This is a filter attribute. Use this attribute to specify the user status for which you want to reconcile user records.</p> <p>If you do not want to use this filter attribute, then specify <code>Nodata</code>.</p> <p>See Also: The "Partial Reconciliation" section on page 3-1</p>	<p>The value can be either the user status or <code>Nodata</code>.</p> <p>The default value is <code>Nodata</code>.</p> <p>The status can be one of the following numbers:</p> <ul style="list-style-type: none"> 0 (Proposed) 1 (Enabled) 2 (Offline) 3 (Obsolete) 4 (Archive) 5 (Delete)
Operator	<p>Specifies the logical operator to be applied to the filter attribute</p> <p>If you do not want to use this filter attribute, then specify <code>None</code>.</p> <p>See Also: The "Partial Reconciliation" section on page 3-1</p>	<p>The value can be one of the following:</p> <ul style="list-style-type: none"> ■ <code>AND</code> ■ <code>OR</code> <p>The default value is <code>AND</code>.</p>

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

3.1.5 Adding Custom Attributes for Reconciliation

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

By default, the attributes listed in the "[Reconciliation Module](#)" section on page 1-2 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for reconciliation as follows:

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

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

1. Determine the Database ID for the attribute that you want to add:
 - a. Open the Remedy Administrator Console.
 - b. Expand **Servers**.
 - c. Double-click **Forms**.
 - d. Double-click the CTM:People form.
 - e. Double-click the field whose Database ID you want to determine.
 - f. On the Database tab, the Database ID of the field is displayed as the value of the ID field.

2. Modify the `attributemapping_recon.properties` file, which is in the `OIM_HOME/xellerate/XLIntegrations/BMC/config` directory.

At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

```
OimAttributeName=Database_ID_in_BMC_Remedi
```

For example:

```
Users.EmailAddress=260000002
```

In this example, `EmailAddress` is the reconciliation field and `260000002` is the equivalent Database ID in BMC Remedy System. As a standard, the prefix "Users ." is added at the start of all reconciliation field names.

3. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:
 - a. Open the Resource Objects form. This form is in the Resource Management folder.
 - b. Click **Query for Records**.
 - c. On the Resource Objects Table tab, double-click the BMCRO resource object to open it for editing.
 - d. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.
 - e. Specify a value for the field name.

You must specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 2.

For example, if you uncomment the `Users.EmailAddress=260000002` line in Step 2, then you must specify `Users.EmailAddress` as the attribute name.
 - f. From the **Field Type** list, select a data type for the field.

For example: `String`
 - g. Save the values that you enter, and then close the dialog box.
 - h. If required, repeat Steps d through g to map more fields.
4. Modify the process definition to include the mapping between the newly added attribute and the corresponding reconciliation field as follows:
 - a. Open the Process Definition form. This form is in the Process Management folder.
 - b. On the Reconciliation Field Mappings tab, click **Add Field Map** to open the Add Reconciliation Field Mapping dialog box.
 - c. Enter the required values, save the values that you enter, and then close the dialog box.
 - d. If required, repeat Steps b and c to map more fields.

3.2 Configuring Provisioning

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

This section discusses the following topics related to configuring provisioning:

- [Compiling Adapters](#)
- [Adding Custom Attributes for Provisioning](#)

3.2.1 Compiling Adapters

Note:

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

You need not perform the procedure to compile adapters if you have performed the procedure described in "[Installing the Connector on Oracle Identity Manager Release 9.1.0 or Later](#)" on page 2-3.

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

See Also: The "[Supported Functionality](#)" section on page 1-5 for a listing of the provisioning functions that are available with this connector

- adpBMCCREATEUSER
- adpBMCUPDATEUSER
- adpBMCUPDATEPASSWORD
- adpBMCDELETEUSER
- adpBMCADDSUPPORTGROUP
- adpBMCDELETESUPPORTGROUP
- adpBMCUPDATEERRORADAPTOR
- adpBMCADDSUPPORTGROUP
- adpBMCATESUPPORTGROUP
- adpBMCDELETESUPPORTGROUP

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

To compile adapters by using the Adapter Manager form:

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

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

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

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

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

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

To view detailed information about an adapter:

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

3.2.2 Adding Custom Attributes for Provisioning

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

By default, the attributes listed in the "[Provisioning Module](#)" section on page 1-4 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning as follows:

See Also: *Oracle Identity Manager Design Console Guide*

1. Determine the Database ID for the attribute that you want to add:
 - a. Open the Remedy Administrator Console.
 - b. Expand **Servers**.
 - c. Double-click **Forms**.
 - d. Double-click the CTM:People form.
 - e. Double-click the field whose Database ID you want to determine.
 - f. On the Database tab, the Database ID of the field is displayed as the value of the ID field.
2. Modify the `attributemapping_prov.properties` file, which is in the `OIM_HOME/xellerate/XLIntegrations/BMC/config` directory.

At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of

the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

```
OimAttributeName=Database_ID_in_BMC_Remedy
```

For example:

```
EmailAddress=260000002
```

In this example, `EmailAddress` is the reconciliation field and `260000002` is the equivalent Database ID in BMC Remedy System.

3. Add a new column in the process form.
 - a. Open the process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
 - b. Click **Create New Version**.
 - c. 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.
 - d. From the **Current Version** list, select the newly created version.
 - e. On the Additional Columns tab, click **Add**.
 - f. Specify the new field name and other values.
4. Add a new variable in the variable list.
 - a. Open the Adapter Factory form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.
 - b. Click the **Query for Records** icon.
 - c. On the Adapter Factory Table tab, double-click the **adpBMCCREATEUSER** adapter from the list.
 - d. On the Variable List tab, click **Add**.
 - e. In the Add a Variable dialog box, specify the required values and then save and close the dialog box.
5. Define an additional adapter task for the newly added variable in the `adpBMCCREATEUSER` adapter.
 - a. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.
 - b. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.
 - c. In the Object Instance Selection dialog box, select **Persistent Instance** and then click **Continue**.
 - d. In the Add an Adapter Factory Task dialog box, specify the task name, select the **setProperty** method from the **Method** list, and then click **Save**.
 - e. Map the application method parameters, and then save and close the dialog box. To map the application method parameters:
 - For the "Output: String Return variable (Adapter Variable)" parameter:
 - i. From the **Map to** list, select **Literal**.
 - ii. From the **Name** list, select **Return variable**.
 - For the "Input: String input (Adapter Variable)" parameter:
 - i. From the **Map to** list, select **Adapter Variables**.

- ii. From the **Name** list, select **Input**.
- For the "Input: String Status (Literal)" parameter:
- i. From the **Map to** list, select **Literal**.
 - ii. From the **Name** list, select **String**.
 - iii. In the **Value** field, enter **Status**.
- For the "Input: String Status (Adapter Variable)" parameter:
- i. From the **Map to** list, select **Adapter Variables**.
 - ii. From the **Name** list, select **Status**.
- f. Repeat Steps b through g to create more adapter tasks.
6. Create an additional adapter task to set the input variable.
- a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.
 - b. On the Adapter Tasks tab, click **Add**.
 - c. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.
 - d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.
7. Map the process form columns and adapter variables for the Create User process task as follows:
- a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.
 - b. Click the **Query for Records** icon.
 - c. On the Process Definition Table tab, double-click the **BMCPROCESS** process.
 - d. On the Tasks tab, double-click the **Create User** task.
 - e. In the Closing Form dialog box, click **Yes**.
 - f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, and then save and close the dialog box. To map an unmapped variable:
 - i. Double-click the row in which **N** is displayed in the Status column. The value **N** signifies that the variable is not mapped.
 - ii. From the **Map to** list in the Edit Data Mapping for Variables dialog box, select **Process Data**.
 - iii. From the **Qualifier** list, select the name of the variable.

Repeat Steps i through iii for all unmapped variables.
- Repeat Steps 1 through 6 if you want to add more attributes.

3.3 Configuring the Connector for Multiple Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of BMC Remedy User Management.

You may want to configure the connector for multiple installations of BMC Remedy User Management. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of BMC Remedy User Management.

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

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

1. Create and configure one resource object for each target system installation.

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

2. Create and configure one IT resource for each resource object.

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

3. Design one process form for each resource object.

The Form Designer form is in the Development Tools folder. The UD_BMC process form is created when you import the connector XML file. You can use this process form as the template for creating the remaining process forms.

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

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

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

- From the **Object Name** lookup field, select the resource object that you create in Step 1.
- From the **Table Name** lookup field, select the process form that you create in Step 3.
- While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.

5. Configure reconciliation for each target system installation. Refer to the "[Configuring Reconciliation](#)" section on page 3-1 for instructions.

The following scheduled tasks are created when you import the connector XML file:

For each target system installation, only the values of the following attributes must be changed:

- TargetRO
- ServerName
- IsTrusted

Set the `IsTrusted` attribute to `YES` for the BMC Remedy User Management installation that you want to designate as a trusted source.

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

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the BMC Remedy User Management installation to which you want to provision the user.

Testing and Troubleshooting

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

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

4.1 Testing the Connector

You can use the testing utility to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.

To use the testing utility:

1. Specify values for the parameters in the `config.properties` file. This file is in the `OIM_HOME/xellerate/XLIntegrations/BMC/test/config` directory.

Note: The parameters in the `config.properties` file are the same as the IT resource parameters.

2. Run one of the following files:

For UNIX:

```
OIM_HOME/xellerate/XLIntegrations/tests/scripts/BMCRemedy.sh
```

For Microsoft Windows

```
OIM_HOME\xellerate\XLIntegrations\tests\scripts\BMCRemedy.bat
```

4.1.1 Testing Partial and Batched Reconciliation

You can test both partial and batched reconciliation, in either trusted source or target resource mode, by specifying values for the following user reconciliation attributes:

- BatchSize
- NoOfBatches
- First Name
- Last Name
- Notification Method

- Status
- Operator

These attributes are described in the "[User Reconciliation Scheduled Tasks](#)" section on page 3-6.

The following is a sample set of values for these attributes:

- BatchSize: 4
- NoOfBatches: 2
- First Name: John
- Last Name: Doe
- Notification Method: Nodata
- Status: 1
- Operator: AND

Suppose you specify these values in the target resource user reconciliation scheduled task. After that task is run, all target system records for which the first name and last name values are John and Doe, respectively, are divided into batches of four records each. Of these batches, the first two are reconciled during the current reconciliation run.

4.2 Troubleshooting Connector Problems

The following table lists solutions to some commonly encountered errors associated with the connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the BMC server.	<ul style="list-style-type: none"> ■ Ensure that the BMC Remedy User Management server is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that values for all the IT resource parameters have been correctly specified.
The Operation Failed message is displayed on the Oracle Identity Manager Administrative and User Console.	<ul style="list-style-type: none"> ■ Ensure that the values for the various attributes do not contain delimiter characters (white space). ■ Ensure that the attribute values do not exceed the allowable length.
The following error is encountered: <code>java.lang.UnsatisfiedLinkError: wrong ELF data format: ELFDATA2MSB</code>	<p>Ensure that you are using the specified shared object (.so) files. These files are platform dependent. For example, .so files for SPARC systems cannot work on x86 systems.</p> <p>See "Copying the External Code Files" on page 2-2 for more information.</p>

Known Issues

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

- **Bug 7207232**

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

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

- **Bug 8203695**

In a non-English environment, some of the text on the Administrative and User Console might appear in English because entries for these text items have not been added in the resource bundles.

To work around this issue, you can create and add entries for these items in the resource bundle that you want to use. See *Oracle Identity Manager Globalization Guide* for more information. When you create entries, you must copy the key for each entry from the resource bundle for English.

- **Bug 8367021**

The following issue is observed during trusted source reconciliation:

If a user is marked as Deleted on the target system and if that user has not been reconciled earlier in Oracle Identity Manager, then the user is created in the Enabled state on Oracle Identity Manager at the end of the reconciliation run.

This problem is automatically resolved at the end of the next reconciliation run. At that time, the status of the user in Oracle Identity Manager is set to Disabled.

A

Attribute Mappings Between Oracle Identity Manager and BMC Remedy User Management

The following table discusses attribute mappings between Oracle Identity Manager and BMC Remedy User Management.

Oracle Identity Manager Attribute	BMC Remedy User Management Attribute	Description
Lookup Fields		
Company	CTM:People.Organization.Company	All company names
Department	CTM:People.Organization.Department	All department names
Organization	CTM:People.Organization.Organization	All organization names
Site Group	SIT:Site Group:Site Group	All site groups name
Region	CTM:Region.Region	All regions
Site	SIT:Site Alias Company LookUp.Site	All sites
Site ID	SIT:Site.Site ID	Site ID for a particular Site, Site Group and Region combination
Support Group Company	CTM:Support Group	Support Group company name
Support Group Organization	CTM:Support Group	Support Group Organization Name
Support Group Name	CTM:Support Group	Support Group Name
Support Group ID	CTM:Support Group	Support Group ID
User Attributes		
Profile Status	CTM:People.Profile Status	Profile Status
ARLicenseType	CTM:People.License Type	License type
Department	CTM:People.Department	Department name
Site	CTM:People.Site	Site
Region	CTM:People.Region	Region
LastName	CTM:People.Last Name	Last name
FirstName	CTM:People.First Name	First name
LoginName	CTM:People.Login Name	Login name

Oracle Identity Manager Attribute	BMC Remedy User Management Attribute	Description
Business Phone	CTM:People.Business	Business Phone number
SupportStaff	CTM:People.Support Staff	Support staff
HourlyRate	CTM:People.Hourly Rate	Hourly rate
Vip	CTM:People.VIP	Very important person
Client Type	CTM:People.Client Type	Type of user (internal or external)
NotificationMethod	CTM:People.Notification Method	Notification method
Email	CTM:People.Email Address	E-mail address
ManagerName	CTM:People.Manager's Name	Manager's name
PrimaryCenterCode	CTM:People.Cost Center Code	Cost center code
Password	CTM:People.Password	Password
Client Sensitivity	CTM:Client Sensitivity	Client Sensitivity
Company	CTM:Company	Company Name
Organization	CTM:Organization	Organization Name
Site ID	CTM:Site ID	Site ID
Support Group ID	CTM:Support Group Association	Support Group ID
Support Group Role	CTM:Support Group Role	Support Group Role
Support Group Association ID	CTM:Support Group Association ID	Support Group Association ID
Support Group Company	CTM:Support Group.Comapany	Support Group Company
Support Group Organization	CTM:Support Group.Organization	Support Group Organization
Support Group Name	CTM:Support Group.Support Group	Support Group

Index

A

Adapter Manager form, 3-10
adapters, compiling, 3-10
additional files, 2-1
Administrative and User Console, 2-7, 3-3, 4-2
architecture of the connector, 1-1
attributes
 lookup fields reconciliation scheduled task, 3-4
 user reconciliation scheduled task, 3-6
attributes mappings, A-1

C

changing input locale, 2-11
clearing server cache, 2-11
compiling adapters, 3-10
configuring
 connector for multiple installations of the target system, 3-14
 Oracle Identity Manager server, 2-11
 target system, 2-9
configuring connector, 3-1
configuring provisioning, 3-10
connector architecture, 1-1
connector configuration, 3-1
connector files and directories
 copying, 2-2, 2-6
 description, 1-6
 destination directories, 2-2, 2-6
 installation directory, 1-6, 2-7
connector installer, 2-3
connector testing, 4-1
connector version number, determining, 1-7
connector XML files
 See XML files
creating scheduled tasks, 3-3

D

defining
 IT resources, 2-5
 scheduled tasks, 3-3
deployment requirements, 2-1
Design Console, 3-3
determining version number of connector, 1-7

E

enabling encryption, 2-9
enabling logging, 2-12
encryption
 enabling, 2-9
 error messages, 2-10
 Remedy, 2-9
errors, 4-2
external code files, 2-1

F

files
 additional, 2-1
 external code, 2-1
 See also XML files
files and directories of the connector
 See connector files and directories
functionality supported, 1-5
functions available, 1-5

G

globalization features, 1-6

I

importing connector XML files, 2-7
input locale changing, 2-11
input locale, changing, 2-11
installing connector, 2-3
IT resources
 BMC, 2-5, 2-7, 3-5
 defining, 2-5
 parameters, 2-5
 types, BMCRemedy, 2-8

K

known issues, 5-1

L

limitations, 5-1
logging enabling, 2-12
lookup fields reconciliation, 1-2

lookup fields reconciliation scheduled task, 3-4

M

mapping between attributes of target system and Oracle Identity Manager, A-1
multilanguage support, 1-6

O

Oracle Identity Manager Administrative and User Console, 2-7, 3-3, 4-2
Oracle Identity Manager Design Console, 3-3
Oracle Identity Manager server, configuring, 2-11

P

parameters of IT resources, 2-5
problems, 4-2
process tasks, 1-5
provisioning
 fields, 1-4
 functions, 1-5
 module, 1-4

R

reconciliation
 functions, 1-5
 lookup fields, 1-2
 module, 1-2
 user, 1-3
Remedy encryption
 configuring, 2-9
requirements for deploying, 2-1

S

scheduled tasks
 attributes, 3-4
 defining, 3-3
 lookup fields reconciliation, 3-4
 trusted source user reconciliation, 3-6
server cache, clearing, 2-11
supported
 functionality, 1-5
 releases of Oracle Identity Manager, 2-1
 target systems, 2-1
supported languages, 1-6

T

target system configuration, 2-9
target system, multiple installations, 3-14
target systems supported, 2-1
testing connector, 4-1
testing the connector, 4-1
testing utility, 4-1
troubleshooting, 4-2

U

user attribute mappings, A-1
user reconciliation, 1-3
 trusted source, 3-6
user reconciliation scheduled task, 3-6

V

version number of connector, determining, 1-7

X

XML files
 description, 1-7
 importing, 2-7