Oracle® Identity Manager

Connector Guide for BMC Remedy User Management

Release 9.0.4

E10151-01

May 2007

ORACLE®

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

E10151-01

Primary Author: Shiladitya Guha

Contributing Authors: Deepa Aswani, Debapriya Datta, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for BMC Remedy User Management provides information about integrating Oracle Identity Manager with BMC Remedy User Management.

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

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for BMC Remedy User Management.

Documentation Accessibility

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

http://www.oracle.com/accessibility/

Accessibility of Code Examples in Documentation

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

Accessibility of Links to External Web Sites in Documentation

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

TTY Access to Oracle Support Services

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

Related Documents

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

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

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

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

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

Conventions

The following text conventions are used in this document:

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

What's New in the Oracle Identity Manager Connector for 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 of the Oracle Identity Manager connector pack.

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

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

See Also: *Oracle Identity Manager Release Notes*

Software Updates

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

Configuring Reconciliation

This release provides features that enable you to customize the reconciliation module. Information about connector customization has been provided in the following sections:

- Batched Reconciliation on page 3-2
- Partial Reconciliation on page 3-1

Configuring Attribute Mappings

The connector is preconfigured to support 36 target system attributes. If required, you can add custom attribute mappings by following the procedure described in the following sections:

- Adding Custom Attributes for Reconciliation on page 3-7

- Adding Custom Attributes for Provisioning on page 3-10

Separate Scheduled Tasks for Trusted and Nontrusted Source Reconciliation

In this release of the connector, there are separate user reconciliation scheduled tasks for trusted and nontrusted source reconciliation. In the "User Reconciliation Scheduled Tasks" section on page 3-5, the attributes of these scheduled tasks are described.

Changes in the IT Resource Definition

The following changes have been made in the "Defining IT Resources" section on page 2-9:

The `IsDebug` parameter has been made redundant by the revised exception logging functionality in this release. This parameter has been removed from the IT resource definition.

The `TimeStamp` parameter has been replaced by the `TrustedTimeStamp` and `NonTrustedTimeStamp` parameters, for trusted and nontrusted source reconciliation respectively.

Enhanced Testing Utility

The testing utility provided with this release automates most of the work involved in postdeployment testing of the connector. Information about the files that constitute the testing utility and the procedure involved in the utility has been included in the following sections:

- Files and Directories That Comprise the Connector on page 1-5
- Step 3: Copying the Connector Files and External Code Files on page 2-4
- Testing the Connector on page 4-1

Documentation-Specific Updates

The following documentation-specific updates have been made in this release of the guide:

- Instructions in the "Determining the Release Number of the Connector" section on page 1-6 have been revised.
- Instructions to enable logging for this connector are given in the "Enabling Logging" section on page 2-6.
- Some of the sections that were in Chapter 2 in earlier releases of this guide have been moved to Chapter 3, "Configuring the Connector".

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for BMC Remedy User Management is used to integrate Oracle Identity Manager with BMC Remedy User Management.

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

This chapter contains the following sections:

- Reconciliation Module
- Provisioning Module
- Supported Functionality
- Multilanguage Support
- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector

Note: At some places in this guide, BMC Remedy User Management has been referred to as the *target system*.

Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager additions 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 Framework 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

Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the following lookup fields:

- Country
- Department
- ManagerName
- PagerSw
- PrimaryCenterCode
- Region
- Site
- State

User Reconciliation

User reconciliation involves reconciling the following fields.

Reconciled Resource Object Fields

The following target system fields are reconciled:

- Status
- ARLicenseType
- Department
- Site
- Region
- FullName
- LastName
- FirstName
- LoginName
- PagerSoftware
- Manager
- SupportStaff
- HourlyRate
- Vip
- Type
- NotificationMethod
- EmailAddress
- ManagerName
- Country
- State
- PrimaryCenterCode

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

Provisioning Module

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

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

For this target system, the following fields are provisioned:

- Status
- ARLicenseType
- Department
- Site
- Region
- FullName
- LastName
- FirstName
- LoginName
- PagerSoftware
- Manager
- SupportStaff
- HourlyRate
- Vip
- Type
- NotificationMethod
- EmailAddress
- ManagerName
- Country
- State

- PrimaryCenterCode
- Password

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 Full Name	Provisioning	Updates the full name 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 Status	Provisioning	Updates the status of a user
Update User Type	Provisioning	Updates the type of a user
Update User VIP Field	Provisioning	Updates the VIP status of a user
Update User Manager Field	Provisioning	Updates the manager code of a user
Update User Notification Method Field	Provisioning	Updates the notification method of a user
Update User Manager Name Field	Provisioning	Updates the name of a user's manager
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 State	Provisioning	Updates the state of a user
Update User Country	Provisioning	Updates the country of a user
Update User Hourly Rate	Provisioning	Updates the hourly rate of a user
Update User CostCentercode	Provisioning	Updates the cost center code of a user
Update User ARLicenseType	Provisioning	Updates the ARLicense type of a user
Reconcile Lookup Field	Reconciliation	Reconciles the lookup fields
Reconcile User Data	Reconciliation	Trusted mode: 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. Nontrusted mode: 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"

Multilanguage Support

The connector supports the following languages:

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

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

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 User Management`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`BMCTrigger/Trigger.txt`	This file contains the SQL code for the trigger that is run on the BMC Remedy database for moving the records of deleted users.
`lib/JavaTask/xlBMCRemedy.jar`	This file contains the class files that are required for provisioning.
`lib/ScheduleTask/xlBMCRemedyRecon.jar`	This file contains the class files that are required for reconciliation.
Files in the `resources` directory	Each of these resource bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.

File in the Installation Media Directory	Description
xml/BMCConnector_DM.xml	This file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Resource object ■ Process form ■ Process definition ■ Process tasks ■ Adapter 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.

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

Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

Before Deployment

To determine the release number of a connector before you deploy it:

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

   `Help Desk/BMC Remedy User Management/lib/JavaTask`

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.

Note: If you maintain a copy of the `xlBMCRemedy.jar` file after deployment, then you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

After Deployment

To determine the release number of a connector that has already been deployed:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

2

Deploying the Connector

Deploying the connector involves the following steps:

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

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	BMC Remedy AR System 6.0

External code files	The following JAR and DLL files from the BMC Remedy Admin Client installation directory:
	`arapi60.jar`
	`aruti160.jar`
	`arapi60.dll`
	`arjni60.dll`
	`arrpc60.dll`
	`arutl60.dll`

Target system user account	User account that is a member of the APP-Administrator group You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-9. If the specified privileges were not assigned to the target system user account, then the following message would be displayed: `You do not have write access.`

Step 2: Configuring the Target System

Configuring the target system involves the following steps:

- Creating the SHR:DeletePeople Form

Creating the SHR:DeletePeople Form

The SHR:DeletePeople form is used to store details of deleted users. This information is required during reconciliation.

You can use the Demo user account to create the SHR:DeletePeople form. Alternatively, you can create a user account that has all the privileges of the Demo user account.

To create the SHR:DeletePeople form:

1. Open the ArAdmin tool.

   Connect to the BMC Remedy User Management server by using the user account created in the preceding section. The password can be left blank.
2. Click **Forms.**
3. Click the **SHR:People** form.
4. Select **Save As** from the File menu, and save this form as **SHR:DeletePeople.**

To create a database trigger for moving deleted user records from the SHR:People form to the SHR:DeletePeople form:

1. Determine the names of the tables for the SHR:People and SHR:DeletePeople forms by running the following SELECT statement on the database created for BMC Remedy.

   ```
   SELECT name,schemaid FROM arschema WHERE name LIKE 'SHR:People';
   ```
2. Log in to the BMC Remedy Database by using SQL*Plus.
3. At the SQL prompt, copy the SQL code from the following file in the installation media directory:

   ```
   BMCTrigger/Trigger.txt
   ```

   This file is mentioned in the "Files and Directories That Comprise the Connector" section on page 1-5.
4. In the SQL code, replace the dummy table names, `57` and `608`, with the table names that you determine by performing Step 1.
5. Run the SQL code to create the trigger.

Enabling Encryption

This section discusses the following topics related to Remedy encryption:

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
Encrypt-Security-Policy: 1	Encryption is required.
Encrypt-Public-Key-Expire: 86400	Public key duration is 1 day (86400 seconds).
Encrypt-Symmetric-Data-Key-Expire: 2700	Symmetric data encryption key duration is 45 minutes (2700 seconds).
Encrypt-Public-Key-Algorithm: 5	Public key encryption key strength is RSA-1024 (Performance Security).
Encrypt-Data-Encryption-Algorithm: 2	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.

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 `Encryption-Public-Key-Algorithm` option in the `ar.cfg` (or `ar.conf`) 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 `Encrypt-Data-Encryption-Algorithm` option in the `ar.cfg` (or `ar.conf`) 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.

Step 3: Copying the Connector Files and External Code 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 User Management`

Refer to the "Files and Directories That Comprise the Connector" section on page 1-5 for more information about these files.

File in the Installation Media Directory	Destination Directory
`BMCTrigger/Trigger.txt`	*OIM_home*`/xellerate/BMCTrigger`
`lib/JavaTask/xlBMCRemedy.jar`	*OIM_home*`/xellerate/JavaTasks`
`lib/ScheduleTask/xlBMCRemedyRecon.jar`	*OIM_home*`/xellerate/ScheduleTask`
Files in the `resources` directory	*OIM_home*`/xellerate/connectorResources`
`xml/BMCConnector_DM.xml`	*OIM_home*`/xlclient`

After you copy the connector files:

1. Copy the following files from the BMC Remedy Admin Client installation directory (for example, `C:\Program Files\AR System`) to the *`OIM_home`*`\xellerate\ThirdParty` directory:

   ```
   arapi60.jar
   arutil60.jar
   arapi60.dll
   arjni60.dll
   arrpc60.dll
   arutl60.dll
   ```

2. Include *`OIM_home`*`\xellerate\ThirdParty` in the `PATH` environment variable.

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

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

Step 4: Configuring the Oracle Identity Manager Server

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

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

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.

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 3: Copying the Connector Files and External Code Files" section on page 2-4, you copy files from the `resources` directory on the installation media 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. If you run the command described in Step 2 as follows, then an exception is thrown:

   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

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 informational messages that highlight the progress of the application at 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 still 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**

  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**

  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

- **OC4J**

  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

Step 5: Importing the Connector XML File

As mentioned in the "Files and Directories That Comprise the Connector" section on page 1-5, 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 locating files is displayed.
4. Locate and open the BMCConnector_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 table in the "Defining IT Resources" section on page 2-9 for information about the values to be specified.
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 Tools Reference Guide* for instructions.

11. Click **View Selections**.

The contents of the XML file are displayed on the Import page. You *may* see a cross-shaped icon along with some nodes. 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.

Defining IT Resources

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

Parameter	Description
UserName	User ID that is used to connect to the target system The default value is Demo.
Password	Password for the user ID that is used to connect to the target system
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 Login Name.
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 nontrusted 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.
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 SHR:DeletePeople.
FormName	Name of the form in the target system from which details of newly created and updated users can be obtained The value is SHR: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

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

3

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

Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager additions 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

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.

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.

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 locating 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**.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 5: Importing the Connector XML File" section on page 2-8, the scheduled tasks for lookup fields, trusted source user, and nontrusted 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. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 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 3-7.

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 nontrusted source.

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: ■ Region ■ Site ■ Department ■ PagerSoftware ■ PrimaryCenterCode ■ ManagerName ■ State ■ Country
`LookUpFieldCode`	Name of the lookup field	The value can be any one of the following: ■ `Lookup.BMC.Region` ■ `Lookup.BMC.Site` ■ `Lookup.BMC.Department` ■ `Lookup.BMC.PagerSw` ■ `Lookup.BMC.PrimaryCenterCode` ■ `Lookup.BMC.ManagerName` ■ `Lookup.BMC.State` ■ `Lookup.BMC.Country`

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

User Reconciliation Scheduled Tasks Depending on whether you want to implement trusted or nontrusted soured 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 nontrusted source 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`
`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 `Yes`. For nontrusted source reconciliation, set the value of this attribute to `No`.
`TargetRO`	Name of the resource object	`BMCRO`
`XellerateOrganisation`	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 `BatchSize` attribute. **See Also:** The "Batched Reconciliation" section on page 3-2	Specify `All` 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 `Nodata`. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be either the first name or `Nodata`. The default value is `Nodata`.
`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 `Nodata`. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be either the last name or `Nodata`. The default value is `Nodata`.

Attribute	Description	Value
`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 `Nodata`. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be either the notification method or `Nodata`. The default value is `Nodata`. The notification method value can be one of the following numbers: ■ 0 (None) ■ 1 (Alert) ■ 2 (Email) ■ 3 (User Default)
`Status`	This is a filter attribute. Use this attribute to specify the user status for which you want to reconcile user records. If you do not want to use this filter attribute, then specify `Nodata`. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be either the user status or `Nodata` The default value is `Nodata`. The status can be one of the following numbers: ■ 0 (Active) ■ 1 (Busy) ■ 2 (On Vacation)
`Operator`	Specifies the logical operator to be applied to the filter attribute If you do not want to use this filter attribute, then specify `None`. **See Also:** The "Partial Reconciliation" section on page 3-1	The value can be one of the following: ■ `AND` ■ `OR` The default value is `AND`.

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

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 1-1 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 SHR: 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_Remedy
   ```

   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.

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. Refer to the "Supported Functionality" section on page 1-4 for a listing of the provisioning functions that are available with this connector.

This section discusses the following topics related to configuring provisioning:

- Compiling Adapters
- Adding Custom Attributes for Provisioning

Compiling Adapters

Note: You must perform this procedure if you want to use the provisioning features of the connector.

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 1-4 for a listing of the provisioning functions that are available with this connector

- adpBMCCREATEUSER
- adpBMCUPDATEUSER
- adpBMCUPDATEPASSWORD
- adpBMCDELETEUSER

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.

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 1-3 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 SHR: 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.

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 Acme 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.

4

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

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.

   See Also: The "Defining IT Resources" section on page 2-9 for information about the parameters in the `config.properties` file

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`

Testing Partial and Batched Reconciliation

You can test both partial and batched reconciliation, in either trusted or nontrusted 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 3-5.

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 nontrusted 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.

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.	■ 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.	■ 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.

5

Known Issues

The following are no known issues related to this release of the connector:

- BMC AR System 6.0 does not support SSL.
- 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 locale and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

A

Attribute Mappings Between Oracle Identity Manager and 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		
Country	SHR:People.Country	All country names
Department	SHR:Location.Department	All department names
ManagerName	SHR:People.Manager's Name	All manager names
PagerSw	SHRCFG:ConfigPager.Pager Software Vendor	All pager software vendors
PrimaryCenterCode	SHR:People.Cost Center Code	All primary center codes
Region	SHR:Location.Region	All regions
Site	SHR:Location.Site	All sites
State	SHR:People.State/Prov	All states
User Attributes		
Status	SHR:People.Status	Status
ARLicenseType	SHR:People.License Type	Licence type
Department	SHR:Location.Department	Department name
Site	SHR:Location.Site	Site
Region	SHR:Location.Region	Region
FullName	SHR:People.Full Name	Full name
LastName	SHR:People.Last Name	Last name
FirstName	SHR:People.First Name	First name
LoginName	SHR:People.Login Name	Login name
Id	SHR:People.Identification Number	Identification number
Phone	SHR:People.Phone Number	Phone number
Fax	SHR:People.Fax Number	Fax number

Oracle Identity Manager Attribute	BMC Remedy User Management Attribute	Description
PagerSW	SHRCFG:ConfigPager.Pager Software Vendor	Pager software vendor
PagerPin	SHR:People.Pager PIN	Pager PIN
OfficeNo	SHR:People.Office Number	Office number
PagerProvider	SHR:People.Service Provider	Service provider
Manager	SHR:People.Manager	Manager
SupportStaff	SHR:People.Support Staff	Support staff
HourlyRate	SHR:People.Hourly Rate	Hourly rate
Vip	SHR:People.VIP	Very important person
AccountingCode	SHR:People.Accounting Number	Accounting Number
Type	SHR:People.Type	Type of user (internal or external)
NotificationMethod	SHR:People.Notification Method	Notification method
Email	SHR:People.Email Address	E-mail address
PagerEmail	SHR:People.Paging Email	Paging e-mail
OptParameter1	SHR:People.OptionalParameter1	Optional Parameter 1
WebPage	SHR:People.Web Page Address	Web page address
ManagerName	SHR:People.Manager's Name	Manager's name
OptParameter2	SHR:People.OptionalParameter2	Optional Parameter 2
PagerPhone	SHR:People.PagerPhone	Pager phone number
Street	SHR:People.AddrLine	Address line
PostalCode	SHR:People.Postal Code	Postal code
City	SHR:People.City Name	City name
Country	SHR:People.Country	Country
State	SHR:People.State/Prov	State or province
PrimaryCenterCode	SHR:People.Cost Center Code	Cost center code
Password	SHR:People.Password	Password

Index

M

O

P

R

S

T

U

V

X