Oracle® Identity Manager

Connector Guide for BMC Remedy User Management

Release 9.0.3

B32348-01

February 2007

ORACLE®

Oracle Identity Manager Connector Guide for BMC Remedy User Management, Release 9.0.3

B32348-01

Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery, Venkatasubramaniam Iyer

Contents

Preface v

Audience v
Documentation Accessibility v
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

Supported Functionality 1-1
Multilanguage Support 1-3
Reconciliation Module 1-3
Lookup Fields Reconciliation 1-3
User Reconciliation 1-3
Provisioning Module 1-4
Files and Directories That Comprise the Connector 1-6
Determining the Release Number of the Connector 1-6

2 Deploying the Connector

Step 1: Verifying Deployment Requirements 2-1
Step 2: Configuring the Target System 2-2
Creating a User 2-2
Creating the SHR:DeletePeople Form 2-2
Enabling Encryption 2-2
Enabling Remedy Encryption 2-3
Configuring Remedy Encryption Products 2-3
AR System Encryption Error Messages 2-4
Step 3: Copying the Connector Files and External Code 2-4
Step 4: Configuring the Oracle Identity Manager Server 2-5
Changing to the Required Input Locale 2-6
Clearing Content Related to Connector Resource Bundles from the Server Cache 2-6
Step 5: Importing the Connector XML File 2-6

Defining IT Resources 2-7
Step 6: Configuring Reconciliation 2-8
Configuring Trusted Source Reconciliation 2-8
Creating the Reconciliation Scheduled Tasks 2-9
Specifying Values for the Scheduled Task Attributes 2-10
Lookup Fields Reconciliation Scheduled Task 2-10
User Reconciliation Scheduled Task 2-11
Step 7: Compiling Adapters 2-11
Configuring the Connector for Multiple Installations of the Target System 2-12

3 Testing and Troubleshooting

Testing the Connector 3-1
Troubleshooting 3-1

4 Known Issues

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

Index

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 9.0.1 connector documentation set, 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 connector and documentation for BMC Remedy User Management in release 9.0.3 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.2 release of this guide for information about updates that were new for the 9.0.2 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 updates made to this release of the connector software.

Enhancement in the Multilanguage Support Feature

In addition to the three languages supported by the earlier release, this release of the connector supports seven new languages. All the supported languages are listed in the "Multilanguage Support" section on page 1-3.

Support for OC4J

Earlier releases of the connector supported the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere

This release of the connector also supports Oracle Containers for J2EE (OC4J).

Documentation-Specific Updates

The following documentation-specific update has been made in this release of the guide:

- In the "Step 7: Compiling Adapters" section on page 2-7, the instruction about restarting the node has been removed from Step 4 of the procedure to compile adapters.

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:

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

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 Phone	Provisioning	Updates the phone number of a user
Update User Fax	Provisioning	Updates the fax number of a user

Function	Type	Description
Update User Office Number	Provisioning	Updates the office number of a user
Update User Pager Fields	Provisioning	Updates the pager fields of a user
Update User Web Page	Provisioning	Updates the URL of the Web page of a user
Update User Street	Provisioning	Updates the street name of a user's address
Update User City	Provisioning	Updates the city of a user's address
Update User Postal Code	Provisioning	Updates the postal code of a user's address
Update User Accounting Code	Provisioning	Updates the accounting code of a user
Update User ID	Provisioning	Updates the ID 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 for information about attribute mappings between Oracle Identity Manager and BMC Remedy User Management

Multilanguage Support

This release of the connector supports the following languages:

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

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

Reconciliation Module

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:

- Status
- ARLicenseType
- Department
- Site
- Region

- FullName
- LastName
- FirstName
- LoginName
- Id
- PhoneNumber
- FaxNumber
- PagerSoftware
- PagerPin
- OfficeNo
- PagerProvider
- Manager
- SupportStaff
- HourlyRate
- Vip
- AccountingCode
- Type
- NotificationMethod
- EmailAddress
- PagerEmail
- OptionalParameter1
- WebPage
- ManagerName
- OptionalParameter2
- PagerPhone
- Street
- PostalCode
- City
- Country
- State
- PrimaryCenterCode

Provisioning Module

The following fields are provisioned:

- Status
- ARLicenseType
- Department

- Site
- Region
- FullName
- LastName
- FirstName
- LoginName
- Id
- PhoneNumber
- FaxNumber
- PagerSoftware
- PagerPin
- OfficeNo
- PagerProvider
- Manager
- SupportStaff
- HourlyRate
- Vip
- AccountingCode
- Type
- NotificationMethod
- EmailAddress
- PagerEmail
- OptionalParameter1
- WebPage
- ManagerName
- OptionalParameter2
- PagerPhone
- Street
- PostalCode
- City
- Country
- State
- PrimaryCenterCode
- Password

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are compressed 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.
`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

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

Determining the Release Number of the Connector

To determine the release number of the connector:

1. Extract the contents of the `xlBMCRemedy.jar` file. This file is in the `lib\JavaTasks` directory inside the installation media directory.
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.

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
- Step 4: Configuring the Oracle Identity Manager Server
- Step 5: Importing the Connector XML File
- Step 6: Configuring Reconciliation
- Step 7: Compiling Adapters

If you want to configure the connector for multiple installations of BMC Remedy User Management, then perform the following procedure:

- Configuring the Connector for Multiple Installations of the Target System

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	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 2-7.

Step 2: Configuring the Target System

Configuring the target system involves the following steps:

- Creating a User
- Creating the SHR:DeletePeople Form
- Enabling Encryption

Creating a User

Use the User form to create a user with `License Type=Fixed`. This user account is used to create new (custom) forms.

Creating the SHR:DeletePeople Form

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

To create the SHR:DeletePeople form:

1. Open the ArAdmin tool.

   Connect to the BMC Remedy User Management server by using the `Demo` user ID. 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 Oracle 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
   ```

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:

- Enabling Remedy Encryption
- Configuring Remedy Encryption Products
- AR System Encryption Error Messages

Enabling Remedy Encryption

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.

Configuring Remedy Encryption Products

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 encryption is enabled, then you can set encryption to `required` or `allowed`. If this option is not in the `ar.cfg` (or `ar.conf`) file, then encryption is disabled by default. You can assign 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.

Sample Encryption Product Settings in the Configuration File

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).

Option Settings	Significance
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.

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

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 1-6 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.

Step 4: 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

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.

To set the required input locale:

Note: Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.
2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the *OIM_home*\xellerate\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.
2. Enter one of the following commands:

Note: You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:

OIM_home\xellerate\bin*batch_file_name*

- On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

- On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

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

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

Step 5: Importing the Connector XML File

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 2-7 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. Remove these nodes 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 "Step 6: Configuring Reconciliation" section on page 2-8.

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`.

Parameter	Description
IsDebug	Specifies whether or not debugging statements must be displayed The value can be YES or NO. The default is NO.
TimeStamp	For the first reconciliation run, specify the value None for this parameter. From the next reconciliation run time onward, this parameter stores the time at which the last reconciliation run was completed. The default value is None.
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.

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

Step 6: Configuring Reconciliation

Configuring reconciliation involves the following steps:

- Configuring Trusted Source Reconciliation
- Creating the Reconciliation Scheduled Tasks

Configuring Trusted Source Reconciliation

Note: Perform this step of the procedure only if you want to configure trusted source reconciliation. Only one connector can be configured for trusted source reconciliation. If you configure trusted source reconciliation for this connector while you have another trusted source configured, then both connector reconciliations would stop working.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

Use the Oracle Identity Manager Design Console to configure trusted source reconciliation as follows:

1. In the Resource Objects form, select the fields that you want to reconcile as follows:
   a. Expand the **Resource Management** folder.
   b. Double-click **Resource Objects**.
   c. Enter Xellerate User in the **Name** field and then click the **Query** icon.
   d. Double-click **Xellerate User** in the list that is displayed.

e. On the Object Reconciliation tab, add reconciliation fields as required. You must add all the reconciliation fields that are required to provide input for mandatory fields on the Xellerate User form, for example, fields such as User Login and First Name. However, you need not specify a value in the Password field, although it is a mandatory field.

2. In the Process Definition form, create reconciliation field mappings as follows:
   a. Expand the **Process Management** folder.
   b. Double-click **Process Definition**.
   c. Enter `Xellerate User` in the **Name** field and then click the **Query** icon.
   d. On the Reconciliation Field Mappings tab, add reconciliation field mappings as required. All the mandatory fields of the User Defined process form must be mapped.
3. In the Reconciliation Rules form, create a rule for the `Xellerate User` object as follows:
   a. Expand the **Development Tools** folder.
   b. Double-click **Reconciliation Rules**.
   c. Create a rule for the Xellerate User object, with a rule element as required.

      See: *Oracle Identity Manager Design Console Guide* for instructions

   d. Select the **Active** check box to enable the rule.

Creating the Reconciliation Scheduled Tasks

Configuring reconciliation involves creating scheduled tasks for lookup fields and user reconciliations. To create 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 2-10 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 define the second scheduled task.

After you define both scheduled tasks, proceed to the "Step 7: Compiling Adapters" section on page 2-11.

Specifying Values for the Scheduled Task Attributes

This section provides information about the attribute values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- User Reconciliation Scheduled Task

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the 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.

Attribute	Description	Value
`ServerName`	Name of the IT resource instance	`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

Attribute	Description	Value
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 Task You must specify values for the following attributes of the user 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.

Attribute	Description	Value
ServerName	Name of the IT resource instance	BMC
IsTrusted	Specifies whether or not reconciliation is to be carried out in trusted mode	YES or NO The default is 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.	Xellerate Users

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

Step 7: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- adpBMCCREATEUSER
- adpBMCUPDATEUSER
- adpBMCUPDATEPASSWORD
- adpBMCDELETEUSER

You must compile these adapters before you can use them to provision accounts on the target system.

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.

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.

   Note: To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

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. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

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

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 `BMC` 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 each process definition, the following steps that you must perform are specific to this procedure:

   - 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 "Step 6: Configuring Reconciliation" section on page 2-8 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

   - 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. You can designate either a single or multiple installations of BMC Remedy User Management as the trusted source. For the remaining BMC Remedy User Management installations, set this attribute to NO.

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.

3

Testing and Troubleshooting

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

- Testing the Connector
- Troubleshooting

Testing the Connector

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

To the troubleshooting utility, in a command window, change to the *OIM_home*\xellerate\JavaTasks directory, in which the xlBMCRemedy.jar file is present. Then, perform the following tests:

- Create a BMC Remedy User Management user as follows:

  ```
  java -jar xlBMCRemedy.jar CREATE serverName portNo userName password formName
  lastname fullname type status supportstaff notificationmethod
  ```

  For example:

  ```
  java -jar xlBMCRemedy.jar CREATE 172.19.16.77 0 Demo "" SHR:People jodoe "john
  doe" 1 1 1 1
  ```

- Update a BMC Remedy User Management user as follows:

  ```
  java -jar xlBMCRemedy.jar UPDATE serverName portNo userName password formName
  ModifiedFieldId NewValue
  ```

- Update the password of a BMC Remedy User Management user as follows:

  ```
  java -jar xlBMCRemedy.jar UPDATEPASSWORD serverName portNo userName password
  formName NewPassword ConfirmPassword
  ```

- Delete a BMC Remedy User Management user as follows:

  ```
  java -jar xlBMCRemedy.jar DELETE serverName portNo userName password formName
  ```

Troubleshooting

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.

4

Known Issues

The following are known issues associated with the connector:

- The Secure Sockets Layer (SSL) feature is not supported by BMC AR System 6.0.
- 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 Parameter1
WebPage	SHR:People.Web Page Address	Web page address
ManagerName	SHR:People.Manager's Name	Manager's name
OptParameter2	SHR:People.OptionalParameter2	Optional Parameter2
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

A

Adapter Factory form, 2-12
Adapter Manager form, 2-12
adapters, compiling, 2-11
additional files, 2-1, 2-5
Administrative and User Console, 2-6, 3-2
attributes
  lookup fields reconciliation scheduled task, 2-10
  user reconciliation scheduled task, 2-11
attributes mappings, A-1

C

changing input locale, 2-5, 2-6
clearing server cache, 2-6
compiling adapters, 2-11
configuring
  connector for multiple installations of the target system, 2-12
  Oracle Identity Manager server, 2-5
  reconciliation, 2-8
  target system, 2-2
connector files and directories
  copying, 2-4
  description, 1-6
  destination directories, 2-4
  installation directory, 1-6, 2-5
connector testing, 3-1
connector version number, determining, 1-6
connector XML files
  See XML files
creating scheduled tasks, 2-8, 2-9

D

defining
  IT resources, 2-7
  scheduled tasks, 2-8, 2-9
deployment requirements, 2-1
Design Console, 2-9
determining version number of connector, 1-6

E

enabling encryption, 2-2
encryption
  enabling, 2-2
  error messages, 2-4
  Remedy, 2-2
  sample settings, 2-3
errors, 3-1
external code files, 2-1, 2-5

F

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

G

globalization features, 1-3

I

importing connector XML files, 2-6
input locale changing, 2-5
input locale, changing, 2-6
issues, 4-1
IT resources
  `BMC`, 2-7, 2-10
  defining, 2-7
  parameters, 2-7
  types, `BMCRemedy`, 2-7

L

limitations, 4-1
lookup fields reconciliation, 1-3
lookup fields reconciliation scheduled task, 2-10

M

mapping between attributes of target system and Oracle Identity Manager, A-1
multilanguage support, 1-3

O

Oracle Identity Manager Administrative and User Console, 2-6, 3-2
Oracle Identity Manager Design Console, 2-9
Oracle Identity Manager server, configuring, 2-5

P

parameters of IT resources, 2-7
problems, 3-1
process tasks, 1-1
provisioning
  fields, 1-4
  functions, 1-1
  module, 1-4

R

reconciliation
  configuring, 2-8
  functions, 1-1
  lookup fields, 1-3
  module, 1-3
  trusted source, 2-8
  user, 1-3
Remedy encryption
  configuring, 2-3
  enabling, 2-3
requirements for deploying, 2-1

S

scheduled tasks
  attributes, 2-10
  defining, 2-8, 2-9
  lookup fields reconciliation, 2-10
  user reconciliation, 2-11
server cache, clearing, 2-6
SHR:DeletePeople form, 2-2
SHR:People form, 2-2
supported
  functionality, 1-1
  releases of Oracle Identity Manager, 2-1
  target systems, 2-1
supported languages, 1-3

T

target system configuration, 2-2
target system, multiple installations, 2-12
target systems supported, 2-1
testing connector, 3-1
testing the connector, 3-1
testing utility, 3-1
troubleshooting, 3-1
trusted source reconciliation, 2-8

U

user attribute mappings, A-1
user reconciliation, 1-3
user reconciliation scheduled task, 2-11

V

version number of connector, determining, 1-6

X

XML files
  copying, 2-5
  description, 1-6
  importing, 2-6