# Oracle® Identity Manager

Connector Guide for BMC Remedy User Management

Release 9.0.1

**B31111-01**

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for BMC Remedy User Management, Release 9.0.1

B31111-01



Primary Authors: Debapriya Datta, Shiladitya Guha

Contributing Authors: Don Gosselin, Lyju Vadassery, Venkatasubramaniam Iyer

# 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:** This is a transitional release following Oracle's acquisition of Thor Technologies. 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 set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade 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 Connector Framework Guide*
- Connector guides for various third-party applications

## 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. |

# 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

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 |
| Update User Office Number | Provisioning | Updates the office number of a user |
| Update User Pager Fields | Provisioning | Updates the pager fields of a user |

| Function | Type | Description |
|---|---|---|
| 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.<br>Nontrusted mode: Reconciles user data from BMC Remedy User Management to Oracle Identity Manager. A user is not created in Oracle Identity Manager. |

# Reconciliation Module

This section describes the elements that the reconciliation module extracts from the target system to construct reconciliation event records.

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 of BMC Remedy User Management.

- Status
- ARLicenseType
- Department
- Site
- Region
- FullName
- LastName
- FirstName
- LoginName
- Id
- PhoneNumber
- FaxNumber
- PagerSoftware
- PagerPin
- Office
- 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
- Office
- 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 ZIP file on the installation media:

`Help Desk\BMC Remedy User Management\BMC Remedy User Management Rev 1.0.0.zip`

These files and directories are listed in the following table.

| File in the Installation Media Directory | Description |
|---|---|
| `xml\BMCConnector_DM.xml` | This file contains the following components of the connector:<br>■ IT resource type<br>■ IT resource<br>■ Resource object<br>■ Process form<br>■ Process definition<br>■ Process tasks<br>■ Pre-populate rules<br>■ Adapter tasks |
| `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. |

| File in the Installation Media Directory | Description |
|---|---|
| `docs\B31111_01.pdf`<br>`docs\html` | These are PDF and HTML versions of this guide, which provides instructions to deploy the connector. |

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.

# 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: Importing the Connector XML File
- Step 5: Configuring Reconciliation
- Step 6: Compiling Adapters

## 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 |
| Target system host platforms | Microsoft Windows |
| External code | The following JAR and DLL files from the BMC Remedy Admin Client installation directory:<br>`arapi60.jar`<br>`arutil60.jar`<br>`arapi60.dll`<br>`arjni60.dll`<br>`arrpc60.dll`<br>`arutl60.dll` |

## Step 2: Configuring the Target System

Perform the following steps to configure the target system:

- Create a User
- Create the SHR:DeletePeople Form
- Enable Encryption

## Create a User

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

## Create the SHR:DeletePeople Form

The SHR:DeletePeople form is used to store the 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.**

A database trigger is used in the database to move all deleted users from the SHR:People form to the SHR:DeletePeople form.

---

**Note:** The table for the SHR:People form is `t57`, and the table for the SHR:DeletePeople form is `t608`. You can retrieve the table name by running the following `SELECT` statement on the database:

```
SELECT name,schemaid FROM arschema WHERE name LIKE 'SHR:People';
```

---

Instructions to create this database trigger in the BMC database are given in Appendix A.

## Enable 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**. Examine the status of each AR System process and, if it is running, then stop it.
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). |
| 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.<br>Install the Remedy Encryption product. |
| 9012 | No encryption license.<br>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.<br>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.<br>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.<br>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 ZIP file on the installation media:

`Help Desk\BMC Remedy User Management\BMC Remedy User Management Rev 1.0.0.zip`

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

| File in the Installation Media Directory | Destination Directory |
|---|---|
| `xml\BMCConnector_DM.xml` | *xellerate_home*`\xlclient` |
| `lib\JavaTask\xlBMCRemedy.jar` | *xellerate_home*`\xellerate\JavaTasks` |
| `lib\ScheduleTask\xlBMCRemedyRecon.jar` | *xellerate_home*`\xellerate\ScheduleTask` |
| `docs\B31111_01.pdf`<br>`docs\html` | *xellerate_home*`\xellerate\docs` |

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 *`xellerate_home`*`\xellerate\ThirdParty` directory:

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

2. Include the path of the following files in the `PATH` environment variable:

   ```
   arapi60.dll
   arjni60.dll
   arrpc60.dll
   arutl60.dll
   ```

3. Include the path of the following files in the `CLASSPATH` environment variable:

   ```
   arapi60.jar
   arutil60.jar
   ```

## Step 4: 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 *`xellerate_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 2-6 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. You must remove these nodes. To do this, right-click each such node, and then select **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 5: Configuring Reconciliation" section on page 2-6.

## Defining IT Resources

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

| Parameter Name | Parameter Description |
|---|---|
| UserName | User ID that is used to connect to the target system<br>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<br>The default value is 0. |
| TrustedField | Unique identification key for searching user records<br>The default value is LoginName. |
| IsDebug | Specifies whether or not debugging statements must be displayed<br>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.<br>The default value is None. |
| IsSecure | Specifies whether or not the encryption feature is enabled<br>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<br>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<br>The value is SHR:People. |

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

# Step 5: Configuring Reconciliation

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. Enter a number in the **Max Retries** field. This number represents the number of times Oracle Identity Manager should attempt to complete the task before assigning the `ERROR` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are cleared.
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 appropriate table in the "Specifying Values for the Scheduled Task Attributes"section on page 2-7 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 6: Compiling Adapters" section on page 2-9.

## 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 Name | 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:<br>■ Region<br>■ Site<br>■ Department<br>■ PagerSoftware<br>■ PrimaryCenterCode<br>■ ManagerName<br>■ State<br>■ Country |
| LookUpFieldCode | Name of the lookup field | The value can be any one of the following:<br>■ Lookup.BMC.Region<br>■ Lookup.BMC.Site<br>■ Lookup.BMC.Department<br>■ Lookup.BMC.PagerSw<br>■ Lookup.BMC.PrimaryCostCenterCode<br>■ Lookup.BMC.ManagerName<br>■ Lookup.BMC.State<br>■ Lookup.BMC.Country |

After you specify values for these scheduled task attributes, go 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 Name | 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<br>The default is NO. |
| TargetRO | Name of the resource object | BMCRO |
| XellerateOrganisation | Default value for the Oracle Identity Manager Organization name<br>This value is used to create the Xellerate User in trusted mode. | Xellerate Users |

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

## Step 6: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file. You must compile these adapters before you can use them to provision accounts on the target system.

- adpBMC
- adpBMCUPDATEUSER
- adpBMCUPDATEPASSWORD
- adpBMCDELETEUSER

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 the **Compile All** option.

   To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select the **Compile Selected** option.
3. Click **Start.** Oracle Identity Manager compiles the adapters that you specify.

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 multiple adapters simultaneously, use the Adapter Manager form. To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about how to use these forms.

# 3

# Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected.

This chapter contains the following sections:



## Running Test Cases

This section provides information about running test cases on the connector.

You can use the troubleshooting utility to directly use the connector for identifying the cause of problems associated with connecting to the target system server and performing basic operations on the target system.

From the `JavaTasks` directory, in which the `xlBMCRemedy.jar` file is present, 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 black "steve
  dock" 1 1 1 1
  ```

- Update a BMC Remedy User Management user as follows:

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

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

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

- Delete a BMC Remedy User Management user as follows:

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

## 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.<br>■ Ensure that Oracle Identity Manager is working (that is, the database is running).<br>■ Ensure that all the adapters have been compiled.<br>■ Examine the Oracle Identity Manager record (from the IT Resources form). Ensure that values for all the IT resource parameters have been correctly specified. |
| Operation Fail 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).<br>■ Ensure that the attribute values do not exceed the allowable length. |

# 4

# Known Issues

The following is a known issue associated with this release of the connector:

The Secure Sockets Layer (SSL) feature is not supported by BMC AR System 6.0.

# A

# Creating a Database Trigger in the BMC Database

To create a database trigger for moving all deleted users from the SHR:People form to the SHR:DeletePeople form, perform the following steps:

1. Log in to SQL*Plus.
2. Copy the following script at the SQL prompt:

```
CREATE or REPLACE TRIGGER trig1
AFTER DELETE ON t57
FOR EACH ROW
BEGIN
INSERT INTO t608
(C1,C2,C3,C4,C5,C6,C7,C8,C102,C109,C115,C179,
C100000106,C100000113,C100000120,C100000121,C100000122,
C200000006,C200000007,C200000012,C230000009,C240000001,
C240000003,C240000004,C240000005,C240000006,C240000007,
C240000008,C240000009,C240000010,C240000011,C240000035,
C240000036,C240000037,C240000038,C240000040V,C240000040C,
C240000040D,C240000040USD,C240000040EUR,C240000040GBP,
C240000040JPY,C240000041,C240000042,C260000000,C260000001,
C260000002,C260000003,C260000004,C260000005,C260000006,
C260000008,C260000009,C260000010,C260000026,C261000002,
C261000008,C261000009,C261000010,C261000011,C300469200,
C300469300,C300495800,C300787900)
VALUES
(:old.C1,:old.C2,:old.C3,:old.C4,:old.C5,:old.C6,
:old.C7,:old.C8,:old.C102,:old.C109,:old.C115,:old.C179,
:old.C100000106,:old.C100000113,:old.C100000120,
:old.C100000121,:old.C100000122,:old.C200000006,
:old.C200000007,:old.C200000012,:old.C230000009,
:old.C240000001,:old.C240000003,:old.C240000004,
:old.C240000005,:old.C240000006,:old.C240000007,
:old.C240000008,:old.C240000009,:old.C240000010,
:old.C240000011,:old.C240000035,:old.C240000036,
:old.C240000037,:old.C240000038,:old.C240000040V,
:old.C240000040C,:old.C240000040D,:old.C240000040USD,
:old.C240000040EUR,:old.C240000040GBP,:old.C240000040JPY,
:old.C240000041,:old.C240000042,:old.C260000000,
:old.C260000001,:old.C260000002,:old.C260000003,
:old.C260000004,:old.C260000005,:old.C260000006,
:old.C260000008,:old.C261000009,:old.C260000010,
:old.C260000026,:old.C261000002,:old.C261000008,
:old.C261000009,:old.C261000010,:old.C261000011,
:old.C300469200,:old.C300469300,:old.C300495800,
```

```
:old.C300787900);
end;
/
```

3. Run the script.

# Index

## S



## T



## U



## X