Oracle® Identity Manager

Connector Guide for BMC Ticket Management

Release 9.0.4

E10393-01

May 2007

ORACLE®

Oracle Identity Manager Connector Guide for BMC Ticket Management, Release 9.0.4

E10393-01

Primary Author: Shiladitya Guha

Contributing Authors: Deepa Aswani, Debapriya Datta, Lyju Vadassery

Contents

3 Configuring Connector Functionality

4 Testing and Troubleshooting

5 Known Issues

A Attribute Mappings Between Oracle Identity Manager and BMC Ticket Management

Index

Preface

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

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 Ticket Management is used to integrate Oracle Identity Manager with BMC Ticket 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:

> **Note:** At some places in this guide, BMC Ticket Management has been referred to as the *target system.*
>
> For this connector, BMC Remedy is treated as a provisioning tool or medium.
>
> In this connector, *target application* refers to the application provisioned indirectly via Remedy's Help desk-based manual/automated processes.

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
- Ticket Reconciliation

Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the following lookup fields:

- Category
- Item
- Type

Ticket Reconciliation

Ticket reconciliation involves reconciling the following fields:

- Summary
- Description
- Category
- Type
- Item
- CaseType
- Login
- Name
- Source
- Status

Provisioning Module

Provisioning involves creating or modifying a Ticket in the Remedy Helpdesk system through Oracle Identity Manager.

Oracle Identity Manager sends basic provisioning information to Remedy for provisioning a ticket. The provisioning connector invokes Remedy to generate a ticket. Provisioning information includes:

- Target application
- Access information for target application modules
- User provisioning information

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

In provisioning, you can specify values for the following fields:

- Description

- Category
- Type
- Item
- CaseType
- Source
- OIMUser ID
- CaseID
- OIMStatus

Supported Functionality

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

Function	Type	Description
Create Ticket	Provisioning	Creates a Ticket
Summary Updated	Provisioning	Updates the Summary of a Ticket
Category Updated	Provisioning	Updates the Category of a Ticket
Type Updated	Provisioning	Updates the Type of a Ticket
Item Updated	Provisioning	Updates the Item of a Ticket
CaseType Updated	Provisioning	Updates the CaseType of a Ticket
Source Updated	Provisioning	Updates the Source of a Ticket
Reconcile Lookup Field	Reconciliation	Reconciles the lookup fields
Reconcile Ticket Data	Reconciliation	Reconciles Ticket data from BMC Ticket Management to Oracle Identity Manager

See Also: Appendix A, "Attribute Mappings Between Oracle Identity Manager and BMC Ticket Management"

Multilanguage Support

The connector supports the following languages:

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

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:

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`lib/JavaTask/xlBMCRemedyTicket.jar`	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/ScheduleTask/xlBMCRemedyTicketRecon.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/BMCTicketConnector_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 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 `xlBMCRemedyTicket.jar` file. This file is in the following directory on the installation media:

   ```
   Help Desk/BMC Ticket Management/BMC Remedy Ticket Management Rev
   9.0.4/lib/JavaTask
   ```

2. Open the `manifest.mf` file in a text editor. The `manifest.mf` file is one of the files bundled inside the `xlBMCRemedyTicket.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 `xlBMCRemedyTicket.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	Create a user in Remedy with all the privileges assigned to the Demo user. You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-8.

Step 2: Configuring the Target System

Configuring the target system involves the following steps:

- Customizing the HPD:HelpDesk Form For the Specific Target Application
- Enabling Encryption

Customizing the HPD:HelpDesk Form For the Specific Target Application

Each target application has custom ticket form in Remedy.

User is required to add fields to provide information on Target Application Name, Access information for target application modules and User specific details on the HPD:HelpDesk Form.

There are two approaches, which can be used for this operation

1. Add the additional Fields on the HPD:HelpDesk Form.
2. Create a View of the HPD:HelpDesk Form and add the additional fields in view.

For more details on how to add fields on HPD:HelpDesk Form and to create a view, refer to *Action request system 6.0 Developing ARSystem Application:Basic*.

Enabling Encryption

This section discusses the following topics related to Remedy encryption:

- Enabling Remedy Encryption
- AR System Encryption Error Messages

Enabling 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.

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.

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.

File in the Installation Media Directory	Destination Directory
lib/JavaTask/xlBMCRemedyTicket.jar	*OIM_home*/xellerate/JavaTasks
lib/ScheduleTask/xlBMCRemedyTicketRecon.jar	*OIM_home*/xellerate/ScheduleTask
Files in the resources directory	*OIM_home*/xellerate/connectorResources
xml/BMCTicketConnector_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

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

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.BMCTicket=*log_level*

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

     For example:

     log4j.logger.Adapter.BMCTicket=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.BMCTicket=*log_level*

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

     For example:

     log4j.logger.Adapter.BMCTicket=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.BMCTicket">
   <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.BMCTicket">
   <priority value="INFO"/>
</category>
```

After you enable logging, the 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.BMCTicket=log_level
```

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

   For example:

```
log4j.logger.Adapter.BMCTicket=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 1-4, 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 BMCTicketConnector_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 2-8 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 Default value is blank.
Host	IP address or computer name of the BMC Ticket Management server
Port	TCP/IP port at which the BMC Ticket Management server is listening The default value is 0.
TimeStamp	Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. 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.
FormName	Name of the form/view in the target system from which details of newly created and updated Ticket can be obtained
Max_Retry	The Maximum no of times the connector tries to connect target system.
Delay	The time gap to connect to Target system when Timeout occurs.

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

3

Configuring Connector Functionality

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

- Configuring Reconciliation
- Configuring Provisioning
- Configuring the Connector for Multiple Target Applications
- Configuring the Connector for Multiple Installations of the Target System

> **Note:** This chapter provides 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

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 the Reconciliation Scheduled Tasks
- Adding Custom Attributes for Reconciliation

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 5: Importing the Connector XML File" section on page 2-7, the scheduled tasks for lookup fields 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 3-2 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 3-3.

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.
- BMC Ticket Reconciliation Scheduled Task

  This section describes attributes of the BMC Ticket reconciliation scheduled task.

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.

Attribute	Description	Value
`ServerName`	Name of the IT resource	`BMCTicket`
`LookUpCode`	Name of the lookup code	The value can be any one of the following: - `Lookup.BMCTKT.Category` - `Lookup.BMCTKT.Type` - `Lookup.BMCTKT.Item`

Attribute	Description	Value
LookUpName	Name of the lookup field	The value can be any one of the following: ■ Category ■ Type ■ Item

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

BMC Ticket 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	BMCTicket
TargetRO	Name of the resource object	BMCTicketRO
BatchSize	Use this attribute to specify the number of records that must be included in each batch.	The default value is 1000.
NoOfBatches	Use this attribute to specify the total number of batches that must be reconciled.	Specify All if you want to reconcile all the batches. This is the default value.
	The number of records in each batch is specified by the BatchSize attribute	Specify an integer value if you want to reconcile only a fixed number of batches.
Status	Use this attribute to specify the Ticket status for which you want to reconcile Tickets.	5 (closed) **Note:** You must not change this value.

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. User is required to add custom attributes specific to the target application. These fields will provide information on Target Application Name, Access information for target application modules, and User specific details. 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:HPD:HelpDesk 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:

   `Ticket.EmailAddress=260000002`

   In this example, `EmailAddress` is the reconciliation field and `261000010` is the equivalent Database ID in BMC Remedy System.
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 `BMCTicketRO` 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 `Ticket.EmailAddress=260000002` line in Step 2, then you must specify `Ticket.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

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

As mentioned earlier in this guide, provisioning involves creating or modifying a Ticket information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-3 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 Oracle Identity Manager for this target system.

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 1-3 for a listing of the provisioning functions that are available with this connector

- adpBMCCREATETICKET
- adpBMCUPDATETICKET

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

By default, the attributes listed in the "Provisioning Module" section on page 1-2 are mapped for provisioning between Oracle Identity Manager and the target system. You needs to map additional target application specific attributes for provisioning as follows:

See Also: *Oracle Identity Manager Design Console Guide*

1. Modify the `attributemapping_prov.properties` file, which is in the *`OIM_home`*`/xellerate/XLIntegrations/BMCTICKET/config` directory. You must add target application specific attributes in this file. The format that you must use is as follows:

   `OimAttributeName=BMCFieldID`

   Note: `BMCFieldID` is the Database ID for the field on the BMC Server.

2. 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.

3. 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 **adpBMCCREATETICKET** 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.

4. Define an additional adapter task for the newly added variable in the `adpBMCCREATETICKET`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.

5. 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**.

6. 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 **BMCTicketProcess** 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 Ticket 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 Target Applications

You can create tickets for multiple target applications on BMC Ticket Management. To extend this feature to provisioning operations performed through Oracle Identity Manager, you can create a resource object, process form, IT resource, and Process definition for each target application.

To configure the connector for a specific target application of BMC Ticket Management:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about each step of the following procedure

1. Create and configure one resource object for the target application. The Resource Objects form is in the Resource Management folder.

   The `BMCTicketRO` 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. For example, if Lotus Notes is the target application, then you can create a resource object for with the name `BMCTicketLotusRO`.

2. Create and configure one IT resource for each resource object. The IT Resources form is in the Resource Management folder. The `BMCTicket` IT resource is created when you import the connector XML file. You can use this IT resource as

the template for creating a new IT resource, of the `BMCRemedyTicket` IT resource type.

3. Design one process form for each resource object. The Form Designer form is in the Development Tools folder. The `UD_BMCTKT` process form is created when you import the connector XML file. You can use this process form as the template for creating a new form for adding target application specific attributes.
4. Create and configure one process definition for each resource object. The Process Definition form is in the Process Management folder. The `BMCTicketProcess` process definition is created when you import the connector XML file. You can use this process definition as the template for creating for a new process definition.

   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.
5. To add custom attributes for provisioning, perform the procedure described in the "Adding Custom Attributes for Provisioning" section on page 3-6.

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 Sun Java System Directory.

You may want to configure the connector for multiple installations of Sun Java System Directory. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Acme Multinational Inc. have their own installations of Sun Java System Directory. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of Sun Java System Directory.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of Sun Java System Directory.

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 IT resource for each target system installation.

   The IT Resources form is in the Resource Management folder. An 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 IT resource type.
2. Configure reconciliation for each target system installation. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that you only need to modify the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.

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

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/BMCTICKET/test/config` directory.

   See Also: The "Defining IT Resources" section on page 2-8 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/BMCTicket.sh`

   For Microsoft Windows

   `OIM_home``\xellerate\XLIntegrations\tests\scripts\BMCTicket.bat`

Testing Partial and Batched Reconciliation

You can test both filter-based and batched reconciliation by specifying values for the following user reconciliation attributes:

- BatchSize
- NoOfBatches
- Status

These attributes are described in the "BMC Ticket Reconciliation Scheduled Task" section on page 3-3:

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

- `BatchSize`: 4
- `NoOfBatches`: 2
- `Status`: 5 (closed)

Suppose you specify these values in the nontrusted user reconciliation scheduled task. After that task is run, all target system records for which the `Login Name` and `Status` values are `John` and `x`, 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 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

There 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 Ticket Management

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

Oracle Identity Manager Attribute	BMC Remedy User Management Attribute	Description
Lookup Fields		
Category	`SHR:Categorization.Category`	All categories
Item	`SHR:Categorization.Item`	All Items
Type	`SHR:Categorization.Type`	All Types
CaseType	`HPD:HelpDesk. CaseType`	All Case Type
Source	`HPD:HelpDesk.Source`	All source
User Attributes		
Summary	`HPD:HelpDesk.Summary`	Summary
Description	`HPD:HelpDesk.Description`	Description
CaseID	`HPD:HelpDesk.CaseID`	CaseID
OIMUserId	HPD:HelpDesk.OIMUserId	OIMUserId
OIMStatus	HPD:HelpDesk.OIMStatus	OIMStatus

Index

O

P

R

S

T

U

V

X