Oracle® Identity Manager

Connector Guide for BMC Remedy Ticket Management

Release 9.0.4

E11222-10

April 2012

ORACLE®

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

E11222-10

Primary Author: Gauhar Khan

Contributing Author: Prakash Hulikere

Contents

3 Using the Connector

4 Extending the Functionality of the Connector

5 Testing and Troubleshooting

6 Known Issues

Index

Preface

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

Audience

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

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit
http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Related Documents

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

For generic information about connectors, see *Oracle Fusion Middleware User's Guide for Oracle Identity Manage*r.

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

http://docs.oracle.com/cd/E11223_01/index.htm

Documentation Updates

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

http://www.oracle.com/technology/documentation/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 Ticket Management?

This chapter provides an overview of the updates made to the software and documentation for the BMC Remedy Ticket Management connector in release 9.0.4.12.

> **Note:** Release 9.0.4.12 of the connector comes after release 9.0.4.5. Release numbers from 9.0.4.6 through 9.0.4.11 have not been used.

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

The following sections discuss software updates:

- Software Updates in Release 9.0.4 and 9.0.4.1
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.12

Software Updates in Release 9.0.4 and 9.0.4.1

The following are software updates in release 9.0.4 and 9.0.4.1:

- Changes in IT Resource Parameters
- Additions to the Known Issues List
- Changes in the Directory Structure for the Connector Installation Files

- Changes in Adapter Names

Changes in IT Resource Parameters

In this release of the connector, the `Host`, `TimeStamp`, `Max_Retry`, and `Delay` BMC IT resource parameters have been removed. The `ServerName`, `LastReconTime`, `NoOfTrials`, `DelayBetweenTrials`, and `FullNameOfUser` IT resource parameters have been added. For more information about parameters of the `BMCTicket` IT resource, refer to the "Defining IT Resources" section on page 2-7.

Additions to the Known Issues List

In the Known Issues list in Chapter 6, "Known Issues", the following item has been added:

"This release of the connector supports only the English language."

Changes in the Directory Structure for the Connector Installation Files

Some changes have been made in the directory structure for the connector installation files. These changes are reflected in the following sections:

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

Changes in Adapter Names

In the "Compiling Adapters" section on page 3-6, the names of the adapters have been modified.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Support for the Connector Installer
- Support for BMC Remedy AR System 7.1
- Extended Multilanguage Support
- Resolved Issues in Release 9.0.4.2

Support for the Connector Installer

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

See "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1" for more information.

Support for BMC Remedy AR System 7.1

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

> **Note:** BMC Remedy AR System 6.0 is desupported from this release onward.

- Lookup Fields Reconciliation
- Ticket Reconciliation

- Provisioning Module

- Supported Functionality

- Verifying Deployment Requirements

- Customizing the HPD:IncidentInterface_Create and HPD:Help Desk Forms for Each Target Application

- Defining IT Resources

- Attribute Mappings Between Oracle Identity Manager and BMC Remedy Ticket Management

Extended Multilanguage Support

From this release onward, the connector supports the 12 languages listed in the "Certified Languages" section.

Resolved Issues in Release 9.0.4.2

The following is a resolved issue in release 9.0.4.2:

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

Software Updates in Release 9.0.4.3

The following is a resolved issue in release 9.0.4.3:

Bug Number	Issue	Resolution
8325232	The connector did not work if you used a BMC Remedy server port other than port 0 for connector operations.	This issue has been resolved. You can now use any BMC Remedy server port (including port 0) for connector operations.

Software Updates in Release 9.0.4.4

The following are resolved issues in release 9.0.4.4:

Bug Number	Issue	Resolution
8469308	If the target system was BMC Remedy 7.1, then no rows were returned from the target system during reconciliation runs. In addition, no error messages were recorded in the log file.	This issue has been resolved. Reconciliation now runs successfully on BMC Remedy 7.1. During a reconciliation run, records of all tickets that are closed (that is, the Status field is set to 5) are fetched into Oracle Identity Manager.
8203695	In a non-English environment, some of the text on the Administrative and User Console might have appeared in English because entries for these text items were not added in the resource bundles.	This issue has been resolved. The text items on the Administrative and User Console that were appearing in English in a non-English environment have been added in the resource bundles. Therefore, these text items are now being displayed in their respective locales instead of English.

Software Updates in Release 9.0.4.5

- Support for Specifying the Target System Date Format
- Resolved Issues in Release 9.0.4.5

Support for Specifying the Target System Date Format

The DateFormat attribute has been added in the reconciliation scheduled task. You can use this attribute to specify the format in which date values are stored on the target system. During reconciliation, this date format is used to validate date values fetched from the target system.

See "BMC Ticket Reconciliation Scheduled Task" for more information.

Resolved Issues in Release 9.0.4.5

The following are issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
8940396	You could not run the scheduled tasks for this connector when the BMC Remedy Ticket Management connector was installed along with this connector.	This issue has been resolved. The scheduled tasks can be run even when the BMC Remedy User Management connector is installed along with this connector.
9060506	Reconciliation did not work if the target system was BMC Remedy AR System 7.1 installed on a computer on which the German-language locale was configured.	This issue has been resolved. Reconciliation works even if the target system is BMC Remedy AR System 7.1 installed on a computer on which the German-language locale is configured. The Lookup.BMCTKT.QueryAttribute lookup definition has been introduced to address this issue. See "Updating the Lookup.BMCTKT.QueryAttribute Lookup Definition" for more information.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 3.5.2, "Request-Based Provisioning" for more information.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Releases 9.0.4.1 and 9.0.4.2

Documentation-Specific Updates in Releases 9.0.4.1 and 9.0.4.2

The following documentation-specific updates have been made in releases 9.0.4.1 and 9.0.4.2:

- In the "Customizing the HPD:IncidentInterface_Create and HPD:Help Desk Forms for Each Target Application" section on page 2-11, the instructions have been revised.

- The limitation that the target system does not support SSL communication has been moved from the "Known Issues" chapter to the "Verifying Deployment Requirements" section.

Documentation-Specific Updates in Release 9.0.4.3

The following are documentation-specific updates in release 9.0.4.3:

- In the Using the Connector chapter, the "Configuring the Connector for Multiple Installations of the Target System" section has been removed. This feature is not supported by default.

- In the "Verifying Deployment Requirements" section, changes have been made in the "Target systems" row.

Documentation-Specific Updates in Release 9.0.4.4

The following are documentation-specific updates in release 9.0.4.4:

- In the "Connector Architecture" section, the overview of the connector architecture has been modified.

- The location for copying the arapi70.jar and arutil70.jar files has been modified in the following sections:
  - Oracle Identity Manager Running on Microsoft Windows
  - Oracle Identity Manager Running on Linux or Solaris

- In the "Known Issues" chapter, the following issue has been removed:

  Bug 8203695

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

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

Documentation-Specific Updates in Release 9.0.4.5

The following are documentation-specific updates in release 9.0.4.5:

From this release onward:

- The minimum certified release of Oracle Identity Manager is release 9.1.0.1.

- The minimum certified release of JDK is release 1.4.2.

See "Verifying Deployment Requirements" for the complete listing of certified components.

Documentation-Specific Updates in Release 9.0.4.12

- Major changes have been made to the structure of the guide. The objective of these changes is to synchronize the guide with the changes made to the connector and to improve the usability of the information provided by the guide.

- In Table 1–1, " Certified Components", the target system version has been updated from AR System 7.x to AR System 7.0 and 7.1.

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 external, identity-aware applications. This guide discusses the connector that enables you to use BMC Remedy AR System as a managed (target) resource for Oracle Identity Manager.

In the account management (target resource) mode of the connector, information about tickets created or modified directly on BMC Remedy System can be reconciled into Oracle Identity Manager. This data is used to provision (assign) tickets to or update tickets already assigned to OIM Users. In addition, you can use Oracle Identity Manager to provision or update tickets assigned to OIM Users. These provisioning operations performed on Oracle Identity Manager translate into the creation of or updates to the corresponding tickets on the target system.

This chapter contains the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "Lookup Definitions Used During Reconciliation and Provisioning"
- Section 1.6, "Connector Objects Used During Target Resource Reconciliation and Provisioning"
- Section 1.7, "Roadmap for Deploying and Using the Connector"

> **Note:** At some places in this guide, ARS Remedy System is also 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.

1.1 Certified Components

Table 1–1 lists the certified components for the connector.

Table 1–1   Certified Components

Component	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager:
	■ Oracle Identity Manager release 9.0.1 through 9.0.3.*x*
	■ Oracle Identity Manager release 9.1.0.1 or later
	Note: In this guide, **Oracle Identity Manager release 9.1.0.***x* has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support.
	■ Oracle Identity Manager 11*g* release 1 (11.1.1)
	Note: In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager 11*g* release 1 (11.1.1).
	The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at
	http://www.oracle.com/technetwork/documentation/oim1014-097544.html
Target systems	BMC Remedy AR System 7.0 and 7.1
	Note: The target system does not support SSL communication.
Target system user account	Create a user in BMC Remedy with all the privileges assigned to the Demo user.
	You provide the credentials of this user account while performing the procedure in one of the following sections:
	■ For Oracle Identity Manager release 9.0.1 through 9.1.0.*x*:
	Section 2.5.2, "Importing the Connector XML File"
	■ For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:
	Section 2.4.3, "Configuring the IT Resource"
JDK	The JDK version can be one of the following:
	■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x*, use JDK 1.4.2 or a later release in the 1.4.2 series.
	■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series.
	■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

This release of the connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German

- Italian

- Japanese

- Korean

- Portuguese (Brazilian)

- Spanish

> **See Also:** One of the following guides for information about supported special characters:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*:
>
>   *Oracle Identity Manager Globalization Guide*
>
> - For Oracle Identity Manager release 11.1.1:
>
>   *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

1.3 Connector Architecture

> **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

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

The primary function of the connector is to create tickets on the target system through Oracle Identity Manager. In other words, ARS Remedy System can be configured to run as a target resource of Oracle Identity Manager. In addition, the connector enables provisioning operations through which ticket data changes are propagated from Oracle Identity Manager to ARS Remedy System.

During reconciliation, using scheduled tasks, the connector fetches into Oracle Identity Manager data about tickets created or modified directly on the target system. It reconciles only records that have been provisioned from Oracle Identity Manager. To achieve this, the OIMUserId custom field is added on the target system HPD:Help Desk Forms.

Provisioning involves creating or modifying a Ticket in the Remedy Helpdesk system (incident module) through Oracle Identity Manager. During provisioning, tickets are created and modified in the HPD:Help Desk Forms of the target system. The connector uses Remedy APIs to connect to the target system and provision tickets.

> **Note:** During provisioning, tickets are created or modified *only* in the incident module. Tickets are not created or modified in the Service Request Module (SRM).

Figure 1–1 shows the architecture of the BMC Remedy Ticket Management connector.

Figure 1–1   Architecture of the BMC Remedy Ticket Management Connector
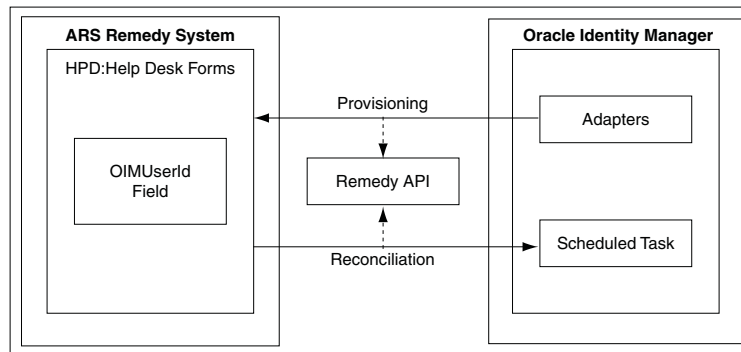
1.4 Features of the Connector

- Section 1.4.1, "Support for Limited Reconciliation"
- Section 1.4.2, "Support for Batched Reconciliation"
- Section 1.4.3, "Support for Both Full and Incremental Reconciliation"
- Section 1.4.4, "Support for Adding New Single-Valued Attributes for Reconciliation and Provisioning"

1.4.1 Support for Limited Reconciliation

You can set a reconciliation filter as the value of the Status attribute of the scheduled task. This filter specifies the subset of newly added and modified target system tickets that must be reconciled.

See Section 3.3.2, "Limited Reconciliation" for more information.

1.4.2 Support for Batched Reconciliation

You can break down a reconciliation run into batches by specifying the number of records that must be included in each batch.

See Section 3.3.3, "Batched Reconciliation" for more information.

1.4.3 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring data of all closed tickets from the target system to Oracle Identity Manager. After the first full reconciliation run, incremental reconciliation is automatically enabled from the next run of the ticket reconciliation.

You can perform a full reconciliation run at any time. See Section 3.3.1, "Full Reconciliation" for more information.

1.4.4 Support for Adding New Single-Valued Attributes for Reconciliation and Provisioning

If you want to add to the standard set of single-valued attributes for reconciliation and provisioning, then perform the procedures described in Chapter 4, "Extending the Functionality of the Connector."

1.5 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during connector operations can be divided into the following categories:

- Section 1.5.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.5.2, "Other Lookup Definitions"

1.5.1 Lookup Definitions Synchronized with the Target System

During a provisioning operation, you use a lookup field on the process form to specify a single value from a set of values. For example, you use the Category lookup field to select the category to which the ticket belongs. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager. Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

The BMCTicket Lookup Reconciliation lookup definition is populated with values fetched from the target system by the scheduled tasks for lookup field synchronization:

> **See Also:** Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about these scheduled tasks

- Lookup.BMCTKT.Category
- Lookup.BMCTKT.Type
- Lookup.BMCTKT.Item

1.5.2 Other Lookup Definitions

Table 1–2 describes the other lookup definitions that are created in Oracle Identity Manager when you deploy the connector. These lookup definitions are either prepopulated with values or values must be manually entered in them after the connector is deployed.

Table 1–2   Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.BMCTKT.ServiceType	This lookup definition contains information about the service types that you can select for a ticket that you create through Oracle Identity Manager.	This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.

Table 1–2 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Lookup.BMCTKT.Urgency	This lookup definition contains information about the urgency that you can select for a ticket that you create through Oracle Identity Manager.	This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.
Lookup.BMCTKT.Impact	This lookup definition contains information about the impact that you can select for a ticket that you create through Oracle Identity Manager.	This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.
Lookup.BMCTKT.ReportedSource	This lookup definition contains information about the reported source that you can select for a ticket that you create through Oracle Identity Manager.	This lookup definition is preconfigured. You cannot add or modify entries in this lookup definition.

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

The following sections provide information about connector objects used during target resource reconciliation and provisioning:

> **See Also:** One of the following guides for conceptual information about reconciliation:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

- Section 1.6.1, "Tickets Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.3, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.4, "Provisioning Functions"

1.6.1 Tickets Attributes for Target Resource Reconciliation and Provisioning

Table 1–3 provides information about user attribute mappings for target resource reconciliation and provisioning.

Table 1–3 Ticket Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Field	Description
Category (Operational Categorization Tier 1)	HPD:Help Desk.Categorization Tier 1	Ticket category
FirstName	HPD:Help Desk.FirstName	First name of the user for whom the ticket is being created.
Impact	HPD:Help Desk.Impact	Incident impact
IncidentId	HPD:Help Desk.IncidentID	Incident ID

Table 1–3   (Cont.) Ticket Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Field	Description
Item (Operational Categorization Tier 3)	HPD:Help Desk.Categorization Tier 2	Item on which the ticket is raised
LastName	HPD:Help Desk.LastName	Last name of the user for whom the ticket is being created.
Notes	HPD:Help Desk.Notes	Any notes or comments pertaining to the ticket
OIMUserId	HPD:Help Desk.OIMUserId	Oracle Identity Manager User ID **Note:** While deploying the connector, you create the OIMUserId field on the target system. During the Create Ticket provisioning operation, this field is populated with the User ID of the OIM User for whom you are creating the ticket. During reconciliation, the value in the OIMUserId field is brought to Oracle Identity Manager and is used for user matching purposes.
ReportedSource	HPD:Help Desk.ReportedSource	Source through which the incident is reported
ServiceType	HPD:Help Desk.ServiceType	Service type
StatusReason	HPD:Help Desk.Resolution	Status reason of the ticket
Summary	HPD:Help Desk.Summary	Ticket summary
Type (Operational Categorization Tier 2)	HPD:Help Desk.Categorization Tier 3	Ticket type
Urgency	HPD:Help Desk.Urgency	Ticket urgency

1.6.2 Reconciliation Rule for Target Resource Reconciliation

> **See Also:**   For generic information about reconciliation matching and action rules, see one of the following guides:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
>
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process-matching rule:

Rule name: BMCTicket Recon Rules

Rule element: User Login equals Ticket.OIMUserId

In this rule:

- User Login is one of the following:

  - For Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*:

    User ID attribute on the Xellerate User form.

  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

User ID attribute on the OIM User form.

■ Ticket.OIMUserId is the OIMUserId attribute of the target system.

After you deploy the connector, you can view the reconciliation rule for target resource reconciliation by performing the following steps:

Note: Perform the following procedure only after the connector is deployed.

---

1. Log in to the Oracle Identity Manager Design Console.

2. Expand **Development Tools**.

3. Double-click **Reconciliation Rules**.

4. Search for **BMCTicket Recon Rules**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2   Reconciliation Rule for Target Resource Reconciliation
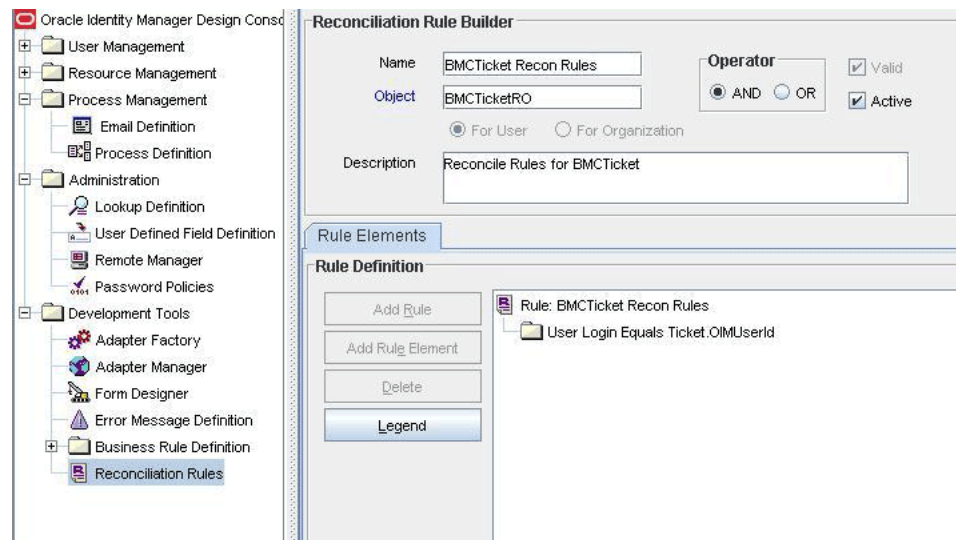
1.6.3 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–4 lists the action rules for target resource reconciliation.

Table 1–4   Action Rules for Target Resource Reconciliation

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See one of the following guides for information about modifying or creating reconciliation action rules:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Design Console*
>
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. Log in to the Oracle Identity Manager Design Console.

2. Expand **Resource Management**.

3. Double-click **Resource Objects**.

4. Search for and open the **BMCTicketRO** resource object.

5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3   Reconciliation Action Rules for Target Resource Reconciliation
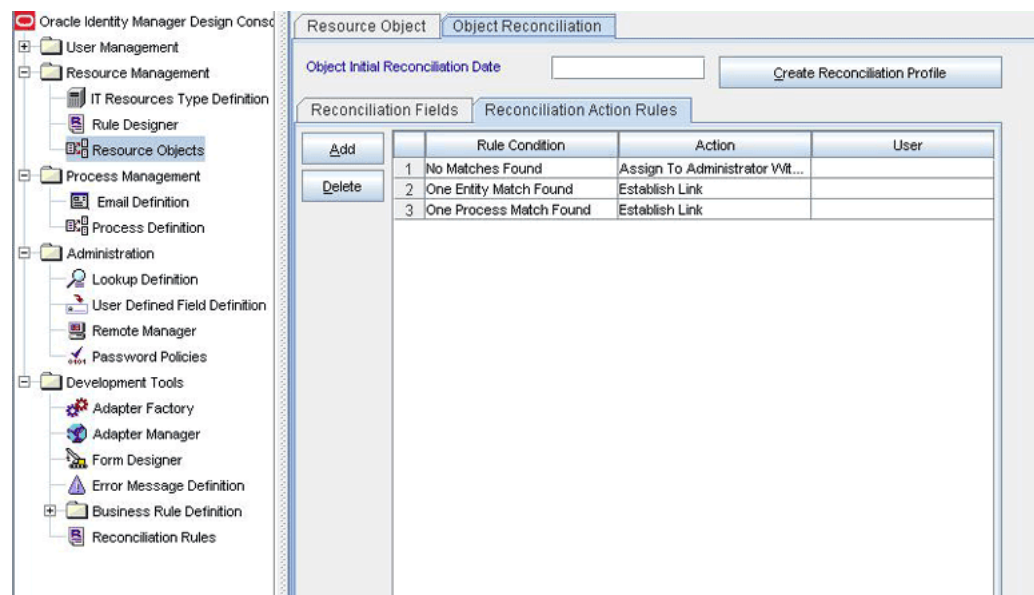
1.6.4 Provisioning Functions

Table 1–5 lists the provisioning functions that are supported by the connector. The Adapter column gives the name of the adapter that is used when the function is performed.

Table 1–5 Provisioning Functions

Function	Adapter
Create Ticket	adpBMCCREATETICKET
Update Summary	adpBMCUPDATETICKET
Update Category	adpBMCUPDATELOOKUPTICKET
Update Type	adpBMCUPDATELOOKUPTICKET
Update Item	adpBMCUPDATELOOKUPTICKET
Update ServiceType	adpBMCUPDATETICKET
Update ReportedSource	adpBMCUPDATETICKET
Update Impact	adpBMCUPDATETICKET

1.7 Roadmap for Deploying and Using the Connector

The following is the organization of information in the rest of this guide:

- Chapter 2, "Deploying the Connector" describes procedures that you must perform on Oracle Identity Manager and the target system during each stage of connector deployment.

- Chapter 3, "Using the Connector" describes the procedure to configure reconciliation runs and perform provisioning operations.

- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.

- Chapter 5, "Testing and Troubleshooting" describes the procedure to use the connector testing utility for testing the connector.

- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2

Deploying the Connector

This chapter is divided into the following sections:

- Section 2.1, "Files and Directories on the Installation Media"
- Section 2.2, "Determining the Release Number of the Connector"
- Section 2.3, "Copying the External Code Files"
- Depending on the release of Oracle Identity Manager that you use, perform the procedures described in one of the following sections:
    - Section 2.4, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"
    - Section 2.5, "Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.x"
- Section 2.6, "Configuring the Target System"
- Section 2.7, "Configuring Oracle Identity Manager"

2.1 Files and Directories on the Installation Media

The files and directories on the installation media are listed and described in Table 2–1.

Table 2–1   Files and Directories On the Installation Media

File in the Installation Media Directory	Description
configuration/BMC RemedyTicket Reconciliation-CI.xml	This XML file contains configuration information that is used during connector installation.
config/attributemapping_prov.properties	This file contains the attributes required for provisioning.
config/attributemapping_recon.properties	This file contains the attributes required for reconciliation.
Files in the dataset directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
lib/xlBMCRemedyTicket.jar	This JAR file contains the class files required for provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database

Table 2–1   (Cont.) Files and Directories On the Installation Media

File in the Installation Media Directory	Description
lib/xlBMCRemedyTicketRecon.jar	This JAR file contains the class files required for reconciliation. During connector installation, this file is copied to the following location:
	■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask
	■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
File in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, these resource bundles are copied to the following location:
	■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources
	■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database
	Note: A **resource bundle** is a file containing localized versions of the text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages.
test/config/config.properties	This file contains the parameters required to connect to the target system and test connector operations.
test/config/log.properties	This file is used to store log information from tests that you run.
test/scripts/BMCRemedyTicket.bat test/scripts/BMCRemedyTicket.sh	This file is used to run the test utility.
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
	■ Lookup definitions
	■ Scheduled tasks

2.2 Determining the Release Number of the Connector

> **Note:**   If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.1 or release 9.1.0.*x*, then the procedure described in this section is optional.
>
> If you are using Oracle Identity Manager release 11.1.1, then skip this section.

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

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

   OIM_HOME/xellerate/JavaTasks/xlBMCRemedyTicket.jar

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.

2.3 Copying the External Code Files

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

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

- Section 2.3.1, "Oracle Identity Manager Running on Microsoft Windows"
- Section 2.3.2, "Oracle Identity Manager Running on Linux or Solaris"

2.3.1 Oracle Identity Manager Running on Microsoft Windows

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

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

2. Copy the following files from the BMC Remedy Admin Client installation directory to the *OIM_HOME*/xellerate/ThirdParty directory for Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, and the *OIM_HOME*/server/ThirdParty directory for Oracle Identity Manager release 11.1.1:

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

   arapi70.dll

   arjni70.dll

   arrpc70.dll

   arutl70.dll

   icudt32.dll

   icuin32.dll

icuuc32.dll

3. Depending on the Oracle Identity Manager release you are using, include one of the following directories in the PATH environment variable:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

  OIM_HOME/xellerate/ThirdParty

- For Oracle Identity Manager release 11.1.1:

  OIM_HOME/server/ThirdParty

2.3.2 Oracle Identity Manager Running on Linux or Solaris

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

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

2. Copy the following files from the BMC Remedy Admin Client installation directory to the *OIM_HOME*/xellerate/ThirdParty directory for Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, and the *OIM_HOME*/server/ThirdParty directory for Oracle Identity Manager release 11.1.1:

   > **Note:** If you do not have these files in your target system installation directory, then check with your vendor.
   >
   > These .so files are different for different (for example, x86 and SPARC) platforms. Ensure that you use the .so files that are specific to the type of platform on which Oracle Identity Manager is running.

   libarjni70.so

   libarutiljni70.so

   libicudatabmc.so

   libicudatabmc.so.32

   libicui18nbmc.so

   libicui18nbmc.so.32

   libicuiobmc.so

   libicuiobmc.so.32

   libicuucbmc.so

   libicuucbmc.so.32

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

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

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

   - For Oracle Identity Manager release 11.1.1:

     ```
     LD_LIBRARY_PATH=OIM_HOME/server/ThirdParty
     ```

```
export LD_LIBRARY_PATH
```

2.4 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.1

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

Installing the connector on Oracle Identity Manager release 9.1.0.*x* or release 11.1.1 involves the following procedures:

- Section 2.4.1, "Running the Connector Installer"
- Section 2.4.2, "Copying Files to the Oracle Identity Manager Host Computer"
- Section 2.4.3, "Configuring the IT Resource"

2.4.1 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

    > **Note:** In an Oracle Identity Manager cluster, copy this JAR file to each node of the cluster.

    - For Oracle Identity Manager release 9.1.0.*x*:
      OIM_HOME/xellerate/ConnectorDefaultDirectory
    - For Oracle Identity Manager release 11.1.1:
      OIM_HOME/server/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:

    - For Oracle Identity Manager release 9.1.0.*x*:

      Oracle Identity Manager Administrative and User Console Guide

    - For Oracle Identity Manager release 11.1.1:

      Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager

3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

    - For Oracle Identity Manager release 9.1.0.*x*:

      Click **Deployment Management**, and then click **Install Connector**.

    - For Oracle Identity Manager release 11.1.1:

      On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.

4. From the Connector List list, select **BMC Remedy Ticket Management** *RELEASE_NUMBER*. This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

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

    a. In the **Alternative Directory** field, enter the full path and name of that directory.

    b. To repopulate the list of connectors in the Connector List list, click **Refresh**.

    c. From the Connector List list, select **BMC Remedy Ticket Management** *RELEASE_NUMBER.*

5. Click **Load**.

6. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

    a. Configuration of connector libraries

    b. Import of the connector XML files (by using the Deployment Manager)

    c. Compilation of adapters

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

    ■ Retry the installation by clicking **Retry.**

    ■ Cancel the installation and begin again from Step 1.

7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

    a. Ensuring that the prerequisites for using the connector are addressed

> **Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.7.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.
>
> There are no prerequisites for some predefined connectors.

    b. Configuring the IT resource for the connector

Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

    c. Configuring the scheduled tasks that are created when you installed the connector

Record the names of the scheduled tasks displayed on this page. The procedure to configure these scheduled tasks is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a clustered environment, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Section 2.1, "Files and Directories on the Installation Media" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.4.2 Copying Files to the Oracle Identity Manager Host Computer

After you run the Connector Installer, you must manually copy the files listed in Table 2–2.

> **Note:** If a particular destination directory does not exist on the Oracle Identity Manager host computer, then create it.

Table 2–2   Files to Be Copied to the Oracle Identity Manager Host Computer

Files on the Installation Media	Destination Directory on the Oracle Identity Manager Release 9.1.0.x Host Computer	Destination Directory on the Oracle Identity Manager Release 11.1.1 Host Computer
Files in the config directory	*OIM_HOME*/xellerate/XLIntegrations/BMCTICKET/config	*OIM_HOME*/server/XLIntegrations/BMCTICKET/config
Files in the test/config directory	*OIM_HOME*/xellerate/XLIntegrations/BMCTICKET/config	*OIM_HOME*/server/XLIntegrations/BMCTICKET/config
Files in the test/scripts directory	*OIM_HOME*/xellerate/XLIntegrations/BMCTICKET/scripts	*OIM_HOME*/server/XLIntegrations/BMCTICKET/scripts

2.4.3 Configuring the IT Resource

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

1. Log in to the Administrative and User Console.

2. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage IT Resource**.

3. If you are using Oracle Identity Manager release 11.1.1, then:

   - On the Welcome page, click **Advanced** in the upper-right corner of the page.

   - On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.

4. In the IT Resource Name field on the Manage IT Resource page, enter `BMCTicket` and then click **Search**.

5. Click the edit icon for the IT resource.

6. From the list at the top of the page, select **Details and Parameters**.

7. Specify values for the parameters of the IT resource. The following table describes each parameter:

Parameter	Description
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
SeverName	IP address or computer name of the BMC Remedy server.
Port	TCP/IP port at which the BMC Remedy server is listening The default value is `0`.
LastReconTime	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`.
FormNameHelpDesk	Name of the form/view in the target system from which details of newly created and updated Ticket can be obtained The default value is `HPD:Help Desk`.
FormNameInterface	Name of the form/view in the target system from which details of newly created tickets can be obtained The default value is `HPD:IncidentInterface_Create`.
NoOfTrials	The maximum number of times the connector tries to connect to the target system. The default value is `2`.
DelayBetweenTrials	The time gap to connect to Target system when timeout occurs. The default value is `2000`.
FullNameOfUser	Full name of the user who is trying to connect to the target system.

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

2.5 Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.*x*

Installing the connector on any Oracle Identity Manager release between releases 9.0.1 and 9.0.3.*x* involves the following procedures:

- Section 2.5.1, "Copying the Connector Files"
- Section 2.5.2, "Importing the Connector XML File"
- Section 2.5.3, "Compiling Adapters"

2.5.1 Copying the Connector Files

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

> **Note:** See Section 2.1, "Files and Directories on the Installation Media" for more information about files in the following table.

File in the Installation Media Directory	Destination Directory
Files in the config directory	*OIM_HOME*/xellerate/XLIntegrations/BMCTICKET/config
Files in the test/config directory	
lib/xlBMCRemedyTicket.jar	*OIM_HOME*/xellerate/JavaTasks
lib/xlBMCRemedyTicketRecon.jar	*OIM_HOME*/xellerate/ScheduleTask
File in the resources directory	*OIM_HOME*/xellerate/connectorResources
Files in the test/scripts directory	*OIM_HOME*/xellerate/XLIntegrations/BMCTICKET/scripts
xml/BMCTicketConnector_DM.xml	*OIM_HOME*/xlclient

2.5.2 Importing the Connector XML File

As mentioned in Section 2.1, "Files and Directories on the Installation Media," the connector XML file contains definitions of the components of the connector. By importing the connector XML file, you create these components in Oracle Identity Manager.

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.

2. Click the **Deployment Management** link on the left navigation bar.

3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.

4. Locate and open the 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 BMCTicket IT resource is displayed.

8. Specify values for the parameters of the BMCTicket IT resource. See Section 2.4.3, "Configuring the IT Resource" for information about the values to be specified.

9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the BMCRemedyTicket IT resource type is displayed.

10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

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

11. Click **View Selections**.

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

12. Click **Import**. The connector XML file is imported into Oracle Identity Manager.

2.5.3 Compiling Adapters

> **Note:** You must perform the procedure described in this section 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:** Section 1.6.4, "Provisioning Functions" for a listing of the provisioning functions that are available with this connector

- adpBMCCreateTicket
- adpBMCUpdateTicket
- adpBMCTKTUserId
- adpBMCUpdateLookupTicket

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.

2.6 Configuring the Target System

Configuring the target system involves the following steps:

- Section 2.6.1, "Customizing the HPD:IncidentInterface_Create and HPD:Help Desk Forms for Each Target Application"

- Section 2.6.2, "Enabling Encryption"

2.6.1 Customizing the HPD:IncidentInterface_Create and HPD:Help Desk Forms for Each Target Application

Each target application must have a custom ticket form in BMC Remedy. To create a custom ticket form for a target application, you can use one of the following methods:

- Create a copy of the **HPD:IncidentInterface_Create** and **HPD:Help Desk** forms.

- Create a view that is based on the **HPD:IncidentInterface_Create and HPD:Help Desk** forms.

Before you create a copy or view of the **HPD:IncidentInterface_Create** or **HPD:Help Desk** form, you must perform the following steps:

> **See Also:** *Action request system 7.1 Developing ARSystem Application:Basic* for more information about adding fields on forms and to create views

1. Add the **OIMUserId** field on the **HPD:IncidentInterface_Create** or **HPD:Help Desk** form as follows:

   a. Log in to BMC Remedy Administrator.

   b. Click **Filters**.

   c. Open the form.

   d. If you are adding the field on the **HPD:Help Desk** form, then click the **Contact** tab.

   e. Create a Character field and place the field as required.

   f. Open the Field Properties dialog box for the character field that you create.

   g. Click the **Display** tab.

   h. In the **Label** field, enter OIMUserID.

   i. Click the **Permissions** tab, and then assign the **Public** permission.

   j. Close the Field Properties page.

   k. Save the changes made to the form.

2. Update the HPD:HII:CreateIncident_100'! filter as follows so that it pushes values from the **HPD: IncidentInerface_Create** form to the **HPD:Help Desk** form:

   a. Log in to BMC Remedy Administrator.

   b. Click **Filters**.

   c. Open the **HPD:HII:CreateIncident_100`!** filter.

   d. Click the If-Action(1) tab.

   e. In the Fields region:

      – From the **Name** menu, select **OIMUserID**.

–   From the **Value** menu, select **OIMUserID**.

f.   Save the filter, and then close it.

3.   Update the value of the **OIMUserId** field in the attributemapping_prov.properties and attributemapping_recon.properties files.

These files are in the following directory:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

    OIM_HOME/xellerate/XLIntegrations/BMCTICKET/config

- For Oracle Identity Manager release 11.1.1:

    OIM_HOME/server/XLIntegrations/BMCTICKET/config

In the attributemapping_prov.properties file, search for the following line:

```
OIMUserId=<database ID>
```

In this line, replace <database ID> with the database ID. For example:

```
OIMUserId=536870915
```

In the attributemapping_recon.properties file, search for the following line:

```
Ticket.OIMUserId=<database ID>
```

In this line, replace <database ID> with the database ID. For example:

```
Ticket.OIMUserId=536870915
```

After you make these changes, create a copy or view of the form for each target system. In each view or copy, add fields to provide information about the following:

- Target application name
- Access information for target application modules
- User-specific details

2.6.2 Enabling Encryption

This section discusses the following topics related to Remedy encryption:

- Section 2.6.2.1, "Enabling Remedy Encryption"
- Section 2.6.2.2, "AR System Encryption Error Messages"

2.6.2.1 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 AR System on the AR server.

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

3. Restart the AR System server.

2.6.2.2 AR System Encryption Error Messages

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

Error Number	Error Message and Description
9010	Encryption is enabled, but the encryption library is not found. Install the Remedy Encryption product.

Error Number	Error Message and Description
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.

2.7 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

- Section 2.7.1, "Changing to the Required Input Locale"
- Section 2.7.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.7.3, "Enabling Logging"
- Section 2.7.4, "Configuring Oracle Identity Manager for Request-Based Provisioning"
- Section 2.7.5, "Updating the Lookup.BMCTKT.QueryAttribute Lookup Definition"

2.7.1 Changing to the Required Input Locale

> **Note:** In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

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

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

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

> **Note:** In an Oracle Identity Manager cluster, you must perform this step on each node of the cluster. Then, restart each node.

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1. Whenever you add a new resource bundle to 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, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.

   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/bin directory.

   > **Note:** You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:
   >
   > For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:
   >
   > *OIM_HOME/xellerate*/bin/*SCRIPT_FILE_NAME*
   >
   > For Oracle Identity Manager release 11.1.1:
   >
   > *OIM_HOME/server*/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

   > **Note:** You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat CATEGORY_NAME` on Microsoft Windows or `PurgeCache.sh CATEGORY_NAME` on UNIX. The `CATEGORY_NAME` argument represents the name of the content category that must be purged.
   >
   > For example, the following commands purge Metadata entries from the server cache:
   >
   > `PurgeCache.bat MetaData`
   >
   > `PurgeCache.sh MetaData`

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

     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. This exception is different from the one mentioned in Step 1.

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

OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

  When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

  `t3://OIM_HOST_NAME:OIM_PORT_NUMBER`

  In this format:

  – Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.

  – Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

2.7.3 Enabling Logging

Depending on the Oracle Identity Manager release you are using, perform the procedure described in one of the following sections:

- Section 2.7.3.1, "Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.x or Release 9.1.0.x"

- Section 2.7.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.7.3.1 Enabling Logging on Oracle Identity Manager Release 9.0.1 through 9.0.3.*x* or Release 9.1.0.*x*

> **Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

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 might 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.

■ **IBM WebSphere Application Server**

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

- **Oracle Application Server**

  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:

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

- **Oracle WebLogic Server**

  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

2.7.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

> **Note:** In an Oracle Identity Manager cluster, perform this procedure on each node of the cluster. Then, restart each node.

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. 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:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

This level enables logging of messages that highlight the progress of the application.

- CONFIG

    This level enables logging of information about fine-grained events that are useful for debugging.

- FINE, FINER, FINEST

    These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in Table 2–3.

Table 2–3   Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

The configuration file for OJDL is logging.xml, which is located at the following path:

DOMAIN_HOME/config/fmwconfig/servers/*OIM_SERVER*/logging.xml

Here, *DOMAIN_HOME* and *OIM_SERVER* are the domain name and server name specified during the installation of Oracle Identity Manager.

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

    a. Add the following blocks in the file:

```
<log_handler name='bmcticket-handler' level='[LOG_LEVEL]'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path' value='[FILE_NAME]'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
  </log_handler>

<logger name="ADAPTER.BMCTICKET" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="bmcticket-handler"/>
     <handler name="console-handler"/>
  </logger>
```

b. Replace both occurrences of **[LOG_LEVEL]** with the ODL message type and level combination that you require. Table 2–3 lists the supported message type and level combinations.

Similarly, replace **[FILE_NAME]** with the full path and name of the log file in which you want log messages to be recorded.

The following blocks show sample values for **[LOG_LEVEL]** and **[FILE_NAME]** :

```
<log_handler name='bmcticket-handler' level='NOTIFICATION:1'
class='oracle.core.ojdl.logging.ODLHandlerFactory'>
<property name='logreader:' value='off'/>
     <property name='path'
value='F:\MyMachine\middleware\user_projects\domains\base_domain1\servers\o
im_server1\logs\oim_server1-diagnostic-1.log'/>
     <property name='format' value='ODL-Text'/>
     <property name='useThreadName' value='true'/>
     <property name='locale' value='en'/>
     <property name='maxFileSize' value='5242880'/>
     <property name='maxLogSize' value='52428800'/>
     <property name='encoding' value='UTF-8'/>
   </log_handler>

<logger name="ADAPTER.BMCTICKET" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="bmcticket-handler"/>
     <handler name="console-handler"/>
   </logger>
```

With these sample values, when you use Oracle Identity Manager, all messages generated for this connector that are of a log level equal to or higher than the NOTIFICATION:1 level are recorded in the specified file.

2. Save and close the file.

3. Set the following environment variable to redirect the server logs to a file:

For Microsoft Windows:

```
set WLS_REDIRECT_LOG=FILENAME
```

For UNIX:

```
export WLS_REDIRECT_LOG=FILENAME
```

Replace *FILENAME* with the location and name of the file to which you want to redirect the output.

4. Restart the application server.

2.7.4 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 and you want to configure request-based provisioning.

In request-based provisioning, an end user raises a ticket request by using the Administrative and User Console. Administrators or other users can also raise ticket

requests for a particular user. Requests for a particular ticket can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (ticket) on the target system.

> **Note:** Direct provisioning allows the provisioning of multiple tickets on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Section 2.7.4.1, "Copying Predefined Request Datasets"
- Section 2.7.4.2, "Importing Request Datasets into MDS"
- Section 2.7.4.3, "Enabling the Auto Save Form Feature"
- Section 2.7.4.4, "Running the PurgeCache Utility"

2.7.4.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following are the predefined request datasets available in the dataset directory on the installation media:

- provisionresource_bmcticketro.xml
- modifyprovisionedresource_bmcticketro.xml

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\BMCTM

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the E:\MyDatasets directory.

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See *Oracle Fusion Middleware Developer's Guide* for Oracle Identity Manager for information on modifying request datasets.

2.7.4.2 Importing Request Datasets into MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

   > **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.7.4.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\BMCTM directory, then set the value of the metada_from_loc property to E:\MyDatasets.

2. In a command window, change to the *OIM_HOME*\server\bin directory.

3. Run one of the following commands:

   - On Microsoft Windows

     `weblogicImportMetadata.bat`

   - On UNIX

     `weblogicImportMetadata.sh`

4. When prompted, enter the following values:

   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to the WebLogic server.

   - `Please enter your server URL [t3://localhost:7001]`

     Enter the URL of the application server in the following format:

     `t3://HOST_NAME_IP_ADDRESS:PORT`

     In this format, replace:

     – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

     – *PORT* with the port on which Oracle Identity Manager is listening.

   The request dataset is imported into MDS.

2.7.4.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.

2. Expand **Process Management,** and then double-click **Process Definition.**

3. Search for and open the **BMCTicketProcess** process definition.

4. Select the **Auto Save Form** check box.

5. Click the Save icon.

2.7.4.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.7.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

2.7.5 Updating the Lookup.BMCTKT.QueryAttribute Lookup Definition

During reconciliation, the scheduled task runs a query (or filter) on the target system to fetch records that meet reconciliation criteria. This filter is based on the Status attribute of the scheduled task and the Last Modified Timestamp parameter of the IT resource. The Lookup.BMCTKT.QueryAttribute lookup definition is used to hold details of this scheduled task attribute and IT resource parameter. The following are the entries in this lookup definition:

Code Key	Decode
Status	ScheduledTask,Status
LastReconTime	ITResource,Last Modified Date,Date

In the second Decode value, Last Modified Date is the name of the target system column. If the name of this column is different on your target system installation, then:

1. On the Design Console, expand the **Administration** folder and then double-click **Lookup Definition**.

2. Search for and open the **Lookup.BMCTKT.QueryAttribute** lookup definition.

3. In the Decode value for **LastReconTime**, make the required change in the column name.

For example, if the name of this column is `Modified On` on your target system, then change the Decode value to the following:

`ITResource,Modified On,Date`

4. Click the Save icon.

3

Using the Connector

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

> **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.

- Section 3.1, "Performing First-Time Reconciliation"
- Section 3.2, "Scheduled Task for Lookup Field Synchronization"
- Section 3.3, "Configuring Reconciliation"
- Section 3.4, "Configuring Scheduled Tasks"
- Section 3.5, "Performing Provisioning Operations"
- Section 3.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1"

3.1 Performing First-Time Reconciliation

First-time reconciliation involves synchronizing lookup definitions in Oracle Identity Manager with the lookup fields of the target system, and performing full reconciliation. In full reconciliation, all existing tickets (of closed status) from the target system are brought into Oracle Identity Manager.

The following is the sequence of steps involved in reconciling all existing tickets:

> **Note:** In Oracle Identity Manager release 11.1.1, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

1. Perform lookup field synchronization by running the scheduled task provided for this operation.

See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about the attributes of the scheduled task for lookup field synchronization.

See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

2. Perform ticket reconciliation by running the scheduled task for ticket reconciliation.

See Section 3.3.4, "Reconciliation Scheduled Task" for information about the attributes of this scheduled task.

See Section 3.4, "Configuring Scheduled Tasks" for information about running scheduled tasks.

After first-time reconciliation, the LastReconTime parameter of the BMCTicket IT resource is automatically set to the time stamp at which the reconciliation run began.

> **See Also:** Section 2.4.3, "Configuring the IT Resource" for information about the parameters of the IT resource

From the next reconciliation run onward, only target system tickets that are closed after the time stamp stored in the IT resource are considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the scheduled task for ticket reconciliation.

3.2 Scheduled Task for Lookup Field Synchronization

The BMCTicket Lookup Reconciliation scheduled task is used for lookup field synchronization.

Table 3–1 describes the attributes of this scheduled task. See Section 3.4, "Configuring Scheduled Tasks" for information about configuring scheduled tasks.

> **Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

Table 3–1 Attributes of the Scheduled Task for Lookup Field Synchronization

Attribute	Description
Server	Enter the name of the target system IT resource.
	Default value: `BMCTicket`
LookupCode	Enter the name of the lookup definition with which values are to be synchronized. You can enter one of the following values:
	■ Lookup.BMCTKT.Category
	■ Lookup.BMCTKT.Type
	■ Lookup.BMCTKT.Item
	There is no default value for this attribute.
LookUpName	Enter the name of the lookup field whose values have to be populated. You can enter one of the following values:
	■ Category
	■ Type
	■ Item
	There is no default value for this attribute.

3.3 Configuring Reconciliation

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

- Section 3.3.1, "Full Reconciliation"

- Section 3.3.2, "Limited Reconciliation"

- Section 3.3.3, "Batched Reconciliation"

- Section 3.3.4, "Reconciliation Scheduled Task"

3.3.1 Full Reconciliation

Full reconciliation involves reconciling all closed tickets from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation. In addition, you can switch from incremental reconciliation to full reconciliation whenever you want to ensure that all target system tickets are reconciled in Oracle Identity Manager.

To perform a full reconciliation run:

- Ensure that the LastReconTime parameter of the BMCTicket IT resource does not contain a value.

- Specify 5 as the value of the Status attribute of the ticket reconciliation scheduled task.

- Specify `All` as the value of the NumberOfBatches attribute of the ticket reconciliation scheduled task.

At the end of the reconciliation run, the LastReconTime parameter of the BMCTicket IT resource is automatically set to the time stamp at which the run started. From the next reconciliation run onward, only tickets created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

3.3.2 Limited Reconciliation

By default, all target system tickets that have been closed after the last reconciliation run are reconciled during the current reconciliation run. In other words, target system tickets that have a status of 5 (closed) are reconciled. You can customize this process by specifying the status of tickets that must be reconciled. You do this by creating filters for the reconciliation module.

For this connector, you create a filter by specifying a value for the Status attribute of the BMCTicket Reconciliation scheduled task while performing the procedure described in Section 3.4, "Configuring Scheduled Tasks."

For example, if you specify 4 as the value of the Status attribute, then all tickets on the target system that have the status Pending are reconciled.

3.3.3 Batched Reconciliation

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

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

- BatchSize: Use this attribute to specify the number of records that must be included in each batch.

- NumberOfBatches: Use this attribute to specify the total number of batches that must be reconciled. If you do not want to use batched reconciliation, specify All as the value of this attribute.

> **Note:** If you specify All as the value of this attribute, then the values of the BatchSize attribute is ignored.

You specify values for these attributes by following the instructions described in Section 3.3.4, "Reconciliation Scheduled Task."

After you configure batched reconciliation, if reconciliation fails during a batched reconciliation run, then refer to the log file for information about the batch at which reconciliation has failed. The log file provides the following information about batched reconciliation:

- Serial numbers of the batches that have been successfully reconciled

- User IDs associated with the records with each batch that has been successfully reconciled

- If the batched reconciliation run fails, then the serial number of the batch that has failed

3.3.4 Reconciliation Scheduled Task

When you run the Connector Installer or import the connector XML file, the BMCTicket Reconciliation scheduled task is automatically created in Oracle Identity Manager. This scheduled task is used to reconcile ticket data from the target system.

You must specify values for the following attributes of the BMCTicket Reconciliation scheduled task. Table 3–2 describes the attributes of this scheduled task. See Section 3.4, "Configuring Scheduled Tasks" for information about configuring scheduled tasks.

> **Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

Table 3–2 Attributes of the Reconciliation Scheduled Task

Attribute	Description
ServerName	Enter the name of the IT resource. Default value: `BMCTicket`
TargetRO	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `BMCTicketRO`
BatchSize	Enter the number of records that must be included in each batch fetched from the target system. Default value: `1000` This attribute is used in conjunction with the NumberOfBatches attribute. All three attributes are discussed in Section 3.3.3, "Batched Reconciliation."
NumberOfBatches	Enter the number of batches that must be reconciled. Default value: `All` Sample value: `50` This attribute is used in conjunction with the BatchSize attribute. All three attributes are discussed in detail in Section 3.3.3, "Batched Reconciliation." If you accept the default value (`All`), then batched reconciliation is not performed.
Status	Specifies the ticket status for which you want to reconcile tickets. Default value: `5` (closed)

3.4 Configuring Scheduled Tasks

You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table 3–3 lists the scheduled tasks that form part of the connector.

Table 3–3 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
BMCTicket Lookup Reconciliation	This scheduled task is used to synchronize the values of the Category, Item, and Type lookup fields between Oracle Identity Manager and the target system. See Section 3.2, "Scheduled Task for Lookup Field Synchronization" for information about this scheduled task.
BMCTicket Reconciliation	This scheduled task is used for ticket reconciliation. See Section 3.3.4, "Reconciliation Scheduled Task" for information about this scheduled task.

Depending on the Oracle Identity Manager release that you are using, perform the procedure described in one of the following sections:

- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.x"

- Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x or Release 11.1.1"

3.4.1 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.*x*

To configure a scheduled task:

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 FAILED status to the task.

6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.

7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.

8. In the Interval region, set the following schedule parameters:

   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option. If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.

   - To set the task to run only once, select the **Once** option.

9. Provide values for the attributes of the scheduled task.

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.

Stopping Reconciliation

Suppose the reconciliation scheduled task for the connector is running and records are being reconciled. If you want to stop the reconciliation process:

1. Perform Steps 1 through 4 of the procedure to configure reconciliation scheduled tasks.

2. Select the **Stop Execution** check box in the task scheduler.

3. Click **Save**.

3.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.*x* or Release 11.1.1

To configure a scheduled task:

1. Log in to the Administrative and User Console.

2. Perform one of the following:

    a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**

    b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.

3. Search for and open the scheduled task as follows:

- If you are using Oracle Identity Manager release 9.1.0.*x*, then:

    a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.

    b. In the search results table, click the edit icon in the Edit column for the scheduled task.

    c. On the Scheduled Task Details page where the details of the scheduled task that you selected is displayed, click **Edit**.

- If you are using Oracle Identity Manager release 11.1.1, then:

    a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.

    b. On the left pane, in the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

    c. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. Modify the details of the scheduled task. To do so:

    a. If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Edit Scheduled Task Details page, modify the following parameters, and then click **Continue**:

      – **Status:** Specify whether you want to leave the task in the enabled state. In the enabled state, the task is ready for use.

      – **Max Retries:** Enter an integer value in this 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. The default value is 1.

      – **Next Start:** Use the date editor to specify the date when you want the task to run. After you select a date value in the date editor, you can modify the time value that is automatically displayed in the Next Start field.

      – **Frequency:** Specify the frequency at which you want the task to run.

    b. If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, you can modify the following parameters:

      – **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

      – **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

> **Note:** See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

In addition to modifying the job details, you can enable or disable a job.

5. Specify values for the attributes of the scheduled task. To do so:

> **Note:** Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.

- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

6. After specifying the attributes, perform one of the following:

- If you are using Oracle Identity Manager release 9.1.0.*x*, then click **Save Changes** to save the changes.

> **Note:** The Stop Execution option is not available in the Administrative and User Console. If you want to stop a task, then click **Stop Execution** on the Task Scheduler form of the Design Console.

- If you are using Oracle Identity Manager release 11.1.1, then click **Apply** to save the changes.

> **Note:** The Stop Execution option is available in the Administrative and User Console. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

3.5 Performing Provisioning Operations

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a ticket on the target system for the user.

When you install the connector on Oracle Identity Manager release 11.1.1, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1."

The following are types of provisioning operations:

- Direct provisioning

- Request-based provisioning

- Provisioning triggered by policy changes

> **See Also:** One of the following guides for information about the types of provisioning
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
>
> - For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

This section discusses the following topics:

- Section 3.5.1, "Direct Provisioning"
- Section 3.5.2, "Request-Based Provisioning"

3.5.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.

2. If you want to first create an OIM User and then provision a ticket on the target system, then:

   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then:

     a. From the Users menu, select **Create**.

     b. On the Create User page, enter values for the OIM User fields and then click **Create User**.

   - If you are using Oracle Identity Manager release 11.1.1, then:

     a. On the Welcome to Identity Administration page, in the Users region, click **Create User**.

     b. On the Create User page, enter values for the OIM User fields, and then click **Save**.

3. If you want to provision a ticket to an existing OIM User, then:

   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then:

     a. From the Users menu, select **Manage**.

     b. Search for the OIM User and select the link for the user from the list of users displayed in the search results.

   - If you are using Oracle Identity Manager release 11.1.1, then:

     a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.

     b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.

4. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then:

     a. On the User Detail page, select **Resource Profile** from the list at the top of the page.

       b. On the Resource Profile page, click **Provision New Resource**.

- If you are using Oracle Identity Manager release 11.1.1, then:

       a. On the user details page, click the **Resources** tab.

       b. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.

5. On the Step 1: Select a Resource page, select **BMCTicketRO** from the list and then click **Continue**.

6. On the Step 2: Verify Resource Selection page, click **Continue**.

7. On the Step 5: Provide Process Data for BMC Remedy Ticket page, specify the required values, and then click **Continue**.

8. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.

9. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:

- If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.

- If you are using Oracle Identity Manager release 11.1.1, then:

       a. Close the window displaying the "Provisioning has been initiated" message.

       b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.2 Request-Based Provisioning

> **Note:** The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1.

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

> **Note:** The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a ticket on the target system. This request is then approved by the approver.

- Section 3.5.2.1, "End User's Role in Request-Based Provisioning"

- Section 3.5.2.2, "Approver's Role in Request-Based Provisioning"

3.5.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

> **See Also:** *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for detailed information about these steps

1. Log in to the Administrative and User Console.

2. On the Welcome page, click **Advanced** in the upper-right corner of the page.

3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.

4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.

5. From the Request Template list, select **Provision Resource** and click **Next**.

6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource (ticket), and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.

7. From the **Available Users** list, select the user to whom you want to provision the resource.

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.

8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.

9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.

10. From the Available Resources list, select **BMCTicketRO**, move it to the Selected Resources list, and then click **Next**.

11. On the Resource Details page, enter details of the ticket that must be created on the target system, and then click **Next**.

12. On the Justification page, you can specify values for the following fields, and then click **Finish**.

    - Effective Date

    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.

13. If you click the request ID, then the Request Details page is displayed.

14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.5.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.

2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.

3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.

4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.

5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.6 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1

> **Note:** It is assumed that you have performed the procedure described in Section 2.7.4, "Configuring Oracle Identity Manager for Request-Based Provisioning."

On Oracle Identity Manager release 11.1.1, if you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.

2. Disable the Auto Save Form feature as follows:

   a. Expand **Process Management**, and then double-click **Process Definition**.

   b. Search for and open the **BMCTicketProcess** process definition.

   c. Deselect the **Auto Save Form** check box.

   d. Click the Save icon.

3. If the Self Request Allowed feature is enabled, then:

   a. Expand **Resource Management**, and then double-click **Resource Objects**.

   b. Search for and open the **BMCTicketRO** resource object.

   c. Deselect the **Self Request Allowed** check box.

   d. Click the Save icon.

On Oracle Identity Manager release 11.1.1, if you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.

2. Enable the Auto Save Form feature as follows:

   a. Expand **Process Management**, and then double-click **Process Definition**.

   b. Search for and open the **BMCTicketProcess** process definition.

   c. Select the **Auto Save Form** check box.

   d. Click the Save icon.

3. If you want to enable end users to raise requests for themselves, then:

   a. Expand **Resource Management**, and then double-click **Resource Objects**.

   b. Search for and open the **BMCTicketRO** resource object.

   c. Select the **Self Request Allowed** check box.

   d. Click the Save icon.

4

Extending the Functionality of the Connector

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

- Section 4.1, "Adding Custom Attributes for Reconciliation"
- Section 4.2, "Adding Custom Attributes for Provisioning"
- Section 4.3, "Configuring the Connector for Multiple Target Applications"

4.1 Adding Custom Attributes for Reconciliation

Note:

- You need not perform this procedure if you do not want to add custom attributes for reconciliation.
- In this section, the term **attribute** refers to the identity data fields that store Ticket data.

By default, the attributes listed in Section 1.6.1, "Tickets Attributes for Target Resource Reconciliation and Provisioning" 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 Ticket specific details. If required, you can map additional attributes for reconciliation as follows:

See Also: One of the following guides for detailed instructions on performing the steps in this section:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

  Oracle Identity Manager Design Console Guide

- For Oracle Identity Manager release 11.1.1:

  Oracle Fusion Middleware Developer's Guide

1. Determine the Database ID for the attribute that you want to add:

   a. Open the Remedy Administrator Console.

   b. Expand **Servers**.

c. Double-click **Forms**.

d. Double-click the **HPD:Help Desk** 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/BMCTICKET/config directory.

Add the new attribute 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 `20000002` is the equivalent Database ID in BMC Remedy System.

3. Log in to the Design Console.

4. 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. Search for and open the **BMCTicketRO** resource object.

c. On the Object Reconciliation tab, click **Add Field** to open the Add Reconciliation Field dialog box.

d. 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 add while performing Step 2.

For example, if you add `Ticket.EmailAddress=260000002` line in Step 2, then you must specify `Ticket.EmailAddress` as the attribute name.

e. From the **Field Type** list, select a data type for the field.

For example: `String`

f. Save the values that you enter, and then close the dialog box.

g. If required, repeat Steps d through g to map more fields.

h. If you are using Oracle Identity Manager release 11.1.1, then click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

5. Add a new field on the process form as follows:

a. Open the Process Forms form. This form is in the Development Tools folder.

b. Search for and open the **UD_BMCTKT** process form.

c. Click **Create New Version**.

d. In the **Label** field of the Create a New Version dialog box, specify a version for the form.

e. Save the changes, and then close the dialog box.

    f. From the **Current Version** list, select the newly created version.

    g. On the Additional Columns tab, click **Add**.

    h. Specify a name and other values for the field. For the example described in Step 4, enter UD_BMCTKT_EMAIL in the Name column and then enter other values for the field.

    i. Click the Save icon.

6. 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. Search for and open the **BMCTicketProcess** process definition.

    c. On the Reconciliation Field Mappings tab, click **Add Field Map** to open the Add Reconciliation Field Mapping dialog box.

    d. Enter the required values, save the values that you enter, and then close the dialog box.

    e. If required, repeat Steps b and c to map more fields.

7. Add the attribute for provisioning. See Section 4.2, "Adding Custom Attributes for Provisioning" for detailed information about the procedure.

4.2 Adding Custom Attributes for Provisioning

> **Note:** In this section, the term **attribute** refers to the identity data fields that store Ticket data.

By default, the attributes listed in Section 1.6.1, "Tickets Attributes for Target Resource Reconciliation and Provisioning" 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:** One of the following guides for detailed instructions on performing the steps in this section:
>
> - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:
>
>   *Oracle Identity Manager Design Console Guide*
>
> - For Oracle Identity Manager release 11.1.1:
>
>   *Oracle Fusion Middleware Developer's 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.

> **Note:** If you have already performed Step 5 of Section 4.1, "Adding
> Custom Attributes for Reconciliation," then directly proceed to Step 3.

   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 a name and other values for the field. For the example described in
      Step 4, enter `UD_BMCTKT_EMAIL`.

   g. Click the Save icon.

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 (for example,
      `Status`) 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 **New Object 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 **Adapter variables**.

      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 the field that you added in the attributemapping_prov.properties file. For example, 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 the field that you added in the attributemapping_prov.properties file. For example, 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 Ticket** 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.

7.   Update the request datasets.

> **Note:** Perform steps 7 through 9 only if you want to perform request-based provisioning.

When you add an attribute on the process form, you also update the XML files containing the request dataset definitions. To update a request dataset:

a. In a text editor, open the XML file located in the *OIM_HOME*/DataSet/file directory for editing.

b. Add the AttributeReference element and specify values for the mandatory attributes of this element.

> **See Also:** The "Configuring Requests" chapter of the *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* guide for more information about creating and updating request datasets

For example, while performing Step 2 of this procedure, if you added E-mail address as an attribute on the process form, then enter the following line:

```
<AttributeReference
name = "E-mail address"
attr-ref = "E-mail address"
type = "String"
widget = "text"
length = "50"
available-in-bulk = "false"/>
```

In this AttributeReference element:

– For the name attribute, enter the value in the Name column of the process form without the tablename prefix.

For example, if UD_BMCTKT_EMAIL is the value in the Name column of the process form, then you must specify `E-mail address` as the value of the name attribute in the AttributeReference element.

– For the attr-ref attribute, enter the value that you entered in the Field Label column of the process form while performing Step 2.

– For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 2.

– For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 2.

– For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 2.

– For the available-in-bulk attribute, specify `true` if the attribute must be available during bulk request creation or modification. Otherwise, specify `false`.

If you added more than one attribute on the process form, then repeat this step for each attribute added.

c. Save and close the XML file.

8. Run the PurgeCache utility to clear content related to request datasets from the server cache.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about the PurgeCache utility.

9. Import into MDS the request dataset definitions in XML format.

   See Section 2.7.4.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

10. If you have not added the attribute for reconciliation, then perform the procedure described in Section 4.1, "Adding Custom Attributes for Reconciliation."

4.3 Configuring the Connector for Multiple Target Applications

You can create tickets for multiple target applications on BMC Remedy Ticket Management. To extend this feature to provisioning operations performed through Oracle Identity Manager, you can apply one of the following approaches:

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

> **See Also:** One of the for detailed information about each step of the following procedure
>
> ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:
>
> *Oracle Identity Manager Design Console Guide*
>
> ■ For Oracle Identity Manager release 11.1.1:
>
> *Oracle Fusion Middleware Developer's Guide*

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 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 Section 4.2, "Adding Custom Attributes for Provisioning."

5

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:

- Section 5.1, "Testing the Connector"
- Section 5.2, "Troubleshooting Connector Problems"

5.1 Testing the Connector

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

To use the testing utility:

1. Specify values for the parameters in the config.properties file. This file is in one of the following directories:

   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*:

     OIM_HOME/xellerate/XLIntegrations/BMCTICKET/test/config

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/XLIntegrations/BMCTICKET/test/config

     See Also: Section 2.4.3, "Configuring the IT Resource" for information about the parameters in the config.properties file

2. Perform one of the following steps:

   - If you are using Oracle Identity Manager release 9.0.1 through 9.0.3.*x* or release 9.1.0.*x*, then run the following script:

     For UNIX:

     OIM_HOME/xellerate/XLIntegrations/tests/scripts/BMCTicket.sh

     For Microsoft Windows:

     OIM_HOME\xellerate\XLIntegrations\tests\scripts\BMCTicket.bat

   - If you are using Oracle Identity Manager release 11.1.1, then run the following script:

     For UNIX:

     OIM_HOME/server/XLIntegrations/tests/scripts/BMCTicket.sh

     For Microsoft Windows:

OIM_HOME\server\XLIntegrations\tests\scripts\BMCTicket.bat

5.1.1 Testing Partial and Batched Reconciliation

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

- BatchSize

- NoOfBatches

These attributes are described in the Section 3.3.4, "Reconciliation Scheduled Task."

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

- BatchSize: 4

- NoOfBatches: 2

Suppose you specify these values in the BMCTicket Reconciliation scheduled task. After that task is run, all target system records are divided into batches of four records each. Of these batches, the first two are reconciled during the current reconciliation run.

5.2 Troubleshooting Connector Problems

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

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the BMC server.	- 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.
The following error is encountered when you perform provisioning or reconciliation: `java.lang.UnsatisfiedLinkError - wrong ELF data format:ELFDATA2MSB`	Ensure that the .so files are compatible to the system where Oracle Identity Manager is deployed. These files are platform dependent. For example, the .so files for SPARC systems cannot work on x86 systems. See Section 2.3, "Copying the External Code Files" for more information.

6

Known Issues

There are no known issues associated with this release of the connector.

Index