Oracle® Identity Manager

Connector Guide for BMC Remedy User Management

Release 9.0.4

E10422-12

July 2014

ORACLE

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

E10422-12

Primary Author: Gowri.G.R

Contributing Authors: Prakash Hulikere, Gauhar Khan, Deena Purushothaman

Contents

Preface ix

Audience ix
Documentation Accessibility ix
Related Documents ix
Documentation Updates ix
Conventions x

What's New in the Oracle Identity Manager Connector for BMC Remedy User Management? xi

Software Updates xi
Documentation-Specific Updates xiv

1 About the Connector

1.1 Certified Components 1-2
1.2 Usage Recommendation 1-2
1.3 Certified Languages 1-3
1.4 Connector Architecture 1-3
1.5 Features of the Connector 1-5
1.5.1 Support for Both Target Resource and Trusted Source Reconciliation 1-5
1.5.2 Support for Limited Reconciliation 1-5
1.5.3 Support for Batched Reconciliation 1-5
1.5.4 Support for Both Full and Incremental Reconciliation 1-5
1.5.5 Support for Adding New Single-Valued Attributes for Reconciliation and Provisioning 1-5
1.6 Lookup Definitions Used During Reconciliation and Provisioning 1-6
1.6.1 Lookup Definitions Synchronized with the Target System 1-6
1.6.2 Other Lookup Definitions 1-6
1.7 Connector Objects Used During Target Resource Reconciliation and Provisioning 1-9
1.7.1 User Attributes for Target Resource Reconciliation and Provisioning 1-10
1.7.2 Support Group Attributes for Target Resource Reconciliation and Provisioning 1-11
1.7.3 Reconciliation Rule for Target Resource Reconciliation 1-11
1.7.4 Reconciliation Action Rules for Target Resource Reconciliation 1-12
1.7.5 Provisioning Functions 1-13
1.8 Connector Objects Used During Trusted Source Reconciliation 1-13
1.8.1 User Attributes for Trusted Source Reconciliation 1-14

1.8.2 Reconciliation Rule for Trusted Source Reconciliation 1-14
1.8.3 Reconciliation Action Rules for Trusted Source Reconciliation 1-15
1.9 Roadmap for Deploying and Using the Connector 1-16

2 Deploying the Connector

2.1 Files and Directories on the Installation Media 2-1
2.2 Determining the Release Number of the Connector 2-2
2.3 Copying the External Code Files 2-3
2.3.1 Oracle Identity Manager Running on Microsoft Windows 2-3
2.3.2 Oracle Identity Manager Running on Linux or Solaris 2-4
2.4 Installing the Connector on Oracle Identity Manager 2-5
2.4.1 Running the Connector Installer 2-5
2.4.2 Copying Files to the Oracle Identity Manager Host Computer 2-7
2.4.3 Configuring the IT Resource 2-8
2.5 Configuring the Target System 2-9
2.5.1 Enabling Encryption 2-9
2.5.1.1 Configuring Remedy Encryption 2-9
2.5.1.2 AR System Encryption Error Messages 2-10
2.6 Configuring Oracle Identity Manager 2-11
2.6.1 Configuring Trusted Source Reconciliation 2-11
2.6.2 Changing to the Required Input Locale 2-12
2.6.3 Clearing Content Related to Connector Resource Bundles from the Server Cache 2-12
2.6.4 Enabling Logging 2-14
2.6.4.1 Enabling Logging on Oracle Identity Manager or Release 9.1.0.*x* 2-14
2.6.4.2 Enabling Logging on Oracle Identity Manager Release 11.1.1 2-16
2.6.5 Configuring Oracle Identity Manager for Request-Based Provisioning 2-18
2.6.5.1 Copying Predefined Request Datasets 2-19
2.6.5.2 Importing Request Datasets into MDS 2-19
2.6.5.3 Enabling the Auto Save Form Feature 2-20
2.6.5.4 Running the PurgeCache Utility 2-20

3 Using the Connector

3.1 Performing First-Time Reconciliation 3-1
3.2 Scheduled Task for Lookup Field Synchronization 3-2
3.3 Configuring Reconciliation 3-5
3.3.1 Full Reconciliation 3-5
3.3.2 Limited Reconciliation 3-6
3.3.3 Batched Reconciliation 3-8
3.3.4 Reconciliation Scheduled Tasks 3-8
3.4 Configuring the Reconciliation Scheduled Tasks 3-11
3.5 Performing Provisioning Operations 3-13
3.5.1 Direct Provisioning 3-14
3.5.2 Request-Based Provisioning 3-15
3.5.2.1 End User's Role in Request-Based Provisioning 3-15
3.5.2.2 Approver's Role in Request-Based Provisioning 3-16
3.6 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1 3-17

4 Extending the Functionality of the Connector

4.1 Adding Custom Attributes for Reconciliation 4-1
4.2 Adding Custom Attributes for Provisioning 4-3
4.3 Configuring the Connector for Multiple Installations of the Target System 4-6

5 Testing and Troubleshooting

5.1 Testing the Connector 5-1
5.1.1 Testing Limited and Batched Reconciliation 5-2
5.2 Troubleshooting Connector Problems 5-2

6 Known Issues

Index

List of Figures

1–1 Architecture of the BMC Remedy User Management Connector 1-4
1–2 Reconciliation Rule for Target Resource Reconciliation 1-12
1–3 Reconciliation Action Rules for Target Resource Reconciliation 1-13
1–4 Reconciliation Rule for Trusted Source Reconciliation 1-15
1–5 Reconciliation Action Rules for Trusted Source Reconciliation 1-16

List of Tables

1–1	Certified Components	1-2
1–2	Other Lookup Definitions	1-7
1–3	User Attributes for Target Resource Reconciliation and Provisioning	1-10
1–4	Support Group Attributes for Target Resource Reconciliation and Provisioning	1-11
1–5	Action Rules for Target Resource Reconciliation	1-12
1–6	Provisioning Functions	1-13
1–7	User Attributes for Trusted Source Reconciliation	1-14
1–8	Action Rules for Target Source Reconciliation	1-15
2–1	Files and Directories On the Installation Media	2-1
2–2	Files to Be Copied to the Oracle Identity Manager Host Computer	2-7
2–3	Log Levels and ODL Message Type:Level Combinations	2-16
3–1	Attributes of the Scheduled Task for Lookup Field Synchronization	3-3
3–2	Attributes of the User Reconciliation Scheduled Tasks	3-9
3–3	Scheduled Tasks for Lookup Field Synchronization and Reconciliation	3-11

Preface

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

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

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

This following sections discuss the software updates:

- Software Updates in Releases 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 Releases 9.0.4 and 9.0.4.1

The following are software updates in releases 9.0.4 and 9.0.4.1:

- Changes in the Directory Structure for the Connector Installation Files

Changes in the Directory Structure for the Connector Installation Files

In this release of the connector, the `BMCTrigger` directory has been changed to the `scripts` directory. Corresponding changes have been made in various sections in this guide.

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
- Additions to the Known Issues List
- 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 Section 2.4, "Installing the Connector on Oracle Identity Manager" 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 various sections in this guide.

Note: BMC Remedy AR System 6.0 is unsupported from this release onward.

Extended Multilanguage Support

From this release onward, the connector supports the 12 languages listed in the "Multilanguage Support" section.

Some of the entries in the resource bundles have not been translated. See the "Known Issues" chapter for more information.

Additions to the Known Issues List

The issue tracked by Bug 8367021 has been added in the "Known Issues" chapter.

Resolved Issues in Release 9.0.4.2

The following are issues resolved 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 Section 2.3, "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

There are no software updates in releases 9.0.4.3.

Software Updates in Release 9.0.4.4

There are no software updates in releases 9.0.4.4.

Software Updates in Release 9.0.4.5

The following are 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 user reconciliation scheduled tasks. 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 "User Reconciliation Scheduled Tasks" 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 Ticket 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.BMC.UM.QueryAttribute and Lookup.BMC.UM.Grp.QueryAttribute lookup definitions have been introduced to address this issue. See Section 3.3.2, "Limited Reconciliation" 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 Release 9.0.4.3
- Documentation-Specific Updates in Release 9.0.4.4
- Documentation-Specific Updates in Release 9.0.4.5
- Documentation-Specific Updates in Release 9.0.4.12

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:

- 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.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target Systems" row.
- The location for copying the arapi70.jar and arutil70.jar files has been modified in the following sections:
  - Section 2.3.1, "Oracle Identity Manager Running on Microsoft Windows"
  - Section 2.3.2, "Oracle Identity Manager Running on Linux or Solaris"

Documentation-Specific Updates in Release 9.0.4.3

There are no documentation-specific updates in release 9.0.4.3.

Documentation-Specific Updates in Release 9.0.4.4

There are no documentation-specific updates in release 9.0.4.4.

Documentation-Specific Updates in Release 9.0.4.5

The following documentation-specific updates have been made 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" section for the complete listing of certified components.

Documentation-Specific Updates in Release 9.0.4.12

The following documentation-specific updates have been made in revision "12" of release 9.0.4.12:

- The "Oracle Identity Manager" row of Table 1–1, " Certified Components" has been modified.
- Section 1.2, "Usage Recommendation" has been added.

The following documentation-specific update has been made in revision "11" of release 9.0.4.12:

Instructions specific to Oracle Identity Manager release 9.0.1 through 9.0.3.*x* have been removed, as these releases are no longer supported.

The following documentation-specific updates have been made in the earlier revisions of the 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 either as a managed (target) resource or as an authoritative (trusted) source of identity data for Oracle Identity Manager.

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

In the identity reconciliation (trusted source) configuration of the connector, users are created or modified only on the target system and information about these users is reconciled into Oracle Identity Manager.

This chapter contains the following sections:

- Section 1.1, "Certified Components"
- Section 1.2, "Usage Recommendation"
- Section 1.3, "Certified Languages"
- Section 1.4, "Connector Architecture"
- Section 1.5, "Features of the Connector"
- Section 1.6, "Lookup Definitions Used During Reconciliation and Provisioning"
- Section 1.7, "Connector Objects Used During Target Resource Reconciliation and Provisioning"
- Section 1.8, "Connector Objects Used During Trusted Source Reconciliation"
- Section 1.9, "Roadmap for Deploying and Using the Connector"

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

At some places in this guide, BMC Remedy System has been referred to as the *target system.* It is used interchangeably with BMC Remedy User Management.

The BMC Remedy User Management connector is also referred to as the user management connector.

1.1 Certified Components

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

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager release 9.1.0.1 and any later BP in this release track **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 supports. ■ Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and any later BP in this release track **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) and future releases in the 11.1.1.*x* series that the connector supports. 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	User account that is a member of the APP-Administrator group You provide the credentials of this user account while defining the IT resource. The procedure is described later in this guide. If the specified privileges were not assigned to the target system user account, then the following message would be displayed: `You do not have write access.`
JDK	The JDK version can be one of the following: ■ 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 Usage Recommendation

Depending on the Oracle Identity Manager version that you are using, you must deploy and use one of the following connectors:

- If you are using an Oracle Identity Manager release that is 9.1.0.1 or later and earlier than Oracle Identity Manager 11*g* Release 1 PS1 (11.1.1.5.7), then use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 PS1 (11.1.1.5.7) or later, or Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later, then use the latest 11.1.1.*x* version of this connector.
- If you are using BMC Remedy AR System 7.0 as the target system, then you must use the 9.0.4.*x* version of this connector.

1.3 Certified Languages

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 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

1.4 Connector Architecture

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

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.

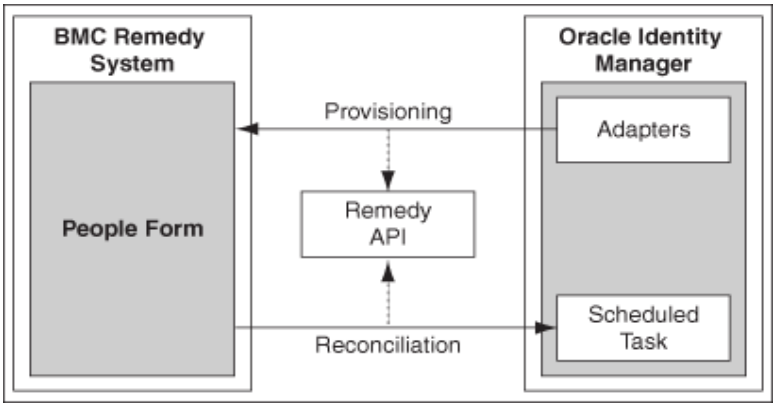
The primary function of a connector is to create Users on the target system through Oracle Identity Manager. The BMC Remedy System (target system) can be configured to run in either the identity reconciliation (trusted source) mode or the provisioning (target resource) mode.

In the identity reconciliation mode, BMC Remedy System is used as the trusted source and users are directly created and modified on it. During reconciliation from the trusted source, the user management connector fetches data (using scheduled task) about these target system users into Oracle Identity Manager. This data is used to create or update the corresponding OIM Users.

In the account management or provisioning mode, BMC Remedy System is used as a target resource. During reconciliation, the user management connector fetches data (using scheduled tasks) about users created or modified directly on the target system into Oracle Identity Manager. This data is used to add or modify resources allocated to OIM Users. In addition, the connector enables provisioning operations through which user data changes are propagated from Oracle Identity Manager to BMC Remedy System.

Figure 1–1 provides the architecture of the BMC Remedy User Management connector.

Figure 1–1 Architecture of the BMC Remedy User Management Connector



Users are created during provisioning in the People form of the BMC Remedy target system. The connector makes use of the Remedy APIs to connect to the Remedy Server, and in turn provision the account.

During reconciliation, scheduled tasks retrieve user records from the People form.

1.5 Features of the Connector

- Section 1.5.1, "Support for Both Target Resource and Trusted Source Reconciliation"
- Section 1.5.2, "Support for Limited Reconciliation"
- Section 1.5.3, "Support for Batched Reconciliation"
- Section 1.5.4, "Support for Both Full and Incremental Reconciliation"
- Section 1.5.5, "Support for Adding New Single-Valued Attributes for Reconciliation and Provisioning"

1.5.1 Support for Both Target Resource and Trusted Source Reconciliation

You can use the connector to configure target system as either a target resource or trusted source of Oracle Identity Manager.

See Section 3.3, "Configuring Reconciliation" for more information.

1.5.2 Support for Limited Reconciliation

You can set a reconciliation filter by specifying values for one or more of the following attributes of the scheduled tasks:

- First Name
- Last Name
- Status
- Notification Method

This filter specifies the subset of newly added and modified target system records that must be reconciled.

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

1.5.3 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.

1.5.4 Support for Both Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data 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 user reconciliation.

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

1.5.5 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."

1.6 Lookup Definitions Used During Reconciliation and Provisioning

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

- Section 1.6.1, "Lookup Definitions Synchronized with the Target System"
- Section 1.6.2, "Other Lookup Definitions"

1.6.1 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 Department lookup field to select a department to which a user must belong to from the list of available departments. 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 following lookup definitions are 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.BMC.Region
- Lookup.BMC.Site
- Lookup.BMC.Department
- Lookup.BMC.Company
- Lookup.BMC.Organization
- Lookup.BMC.SiteGroup
- Lookup.BMC.SiteID
- Lookup.BMC.SupportCompany
- Lookup.BMC.SupportOrganization
- Lookup.BMC.SupportGroup
- Lookup.BMC.RelationshipRole
- Lookup.BMC.SupportGroupID
- Lookup.BMC.PrimaryCentercode
- Lookup.BMC.PagerSw

1.6.2 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.BMC.UM.Grp.QueryAttribute	This lookup definition holds information about filter attributes for group reconciliation.	This lookup definition is preconfigured. You can add entries in this lookup definition, but you must not modify existing entries. See Section 3.3.2, "Limited Reconciliation" for more information about adding entries.
Lookup.BMC.UM.QueryAttribute	This lookup definition holds information about filter attributes for user reconciliation.	This lookup definition is preconfigured. You can add entries in this lookup definition, but you must not modify existing entries. See Section 3.3.2, "Limited Reconciliation" for more information about adding entries.
Lookup.BMC.RelationshipRole	This lookup definition holds information about the relationship roles that you can select for a target system account that you create through Oracle Identity Manager. The following is the format of the Code Key and Decode values in this lookup definition: ■ Code Key: Relationship role name on the target system ■ Decode: Corresponding relationship role name to be displayed in the Relationship Role lookup field of the OIM User form	This lookup definition is preconfigured. You can add or modify entries in this lookup definition if you add or modify entries in the Relationship Role lookup field on the target system See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager 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 for Oracle Identity Manager*
Combo.BMC.ClientType	This lookup definition holds information about client types that you can select for a target system account that you create through Oracle Identity Manager The following is the format of the Code Key and Decode values in this lookup definition: ■ Code Key: Type of client on the target system ■ Decode: Corresponding client type to be displayed in the Client Type field of the OIM User form	This lookup definition is preconfigured. You can add or modify entries in this lookup definition if you add or modify entries in the Client Type field on the target system See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager 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 for Oracle Identity Manager*

Table 1–2 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Combo.BMC.ProfileStatus	This lookup definition holds information about profile statuses that you can select for a target system account that you create through Oracle Identity Manager. The following is the format of the Code Key and Decode values in this lookup definition: ■ Code Key: Profile status name on the target system ■ Decode: Corresponding profile status name to be displayed in the Profile Status field of the OIM User form	This lookup definition is preconfigured. You can add or modify entries in this lookup definition if you add or modify entries in the Profile Status field on the target system See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager 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 for Oracle Identity Manager*
Combo.BMC.ClientSensitivity	This lookup definition holds information about the sensitivity that you can select for a target system account that you create through Oracle Identity Manager. The following is the format of the Code Key and Decode values in this lookup definition: ■ Code Key: Client sensitivity value on the target system ■ Decode: Corresponding client sensitivity value to be displayed in the Sensitivity field of the OIM User form	This lookup definition is preconfigured. You can add or modify entries in this lookup definition if you add or modify entries in the Client Sensitivity field on the target system See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager 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 for Oracle Identity Manager*
Combo.BMC.VIP	You use this lookup definition to specify whether the user is a V.I.P.	This lookup definition is preconfigured. You must not modify the entries in this lookup definition.
Combo.BMC.ARLicenseType	This lookup definition holds information about license types that you can select for a target system account that you create through Oracle Identity Manager. The following is the format of the Code Key and Decode values in this lookup definition: ■ Code Key: License type value on the target system ■ Decode: Corresponding license type value to be displayed in the ARLicenseType field of the OIM User form	This lookup definition is preconfigured. You can add or modify entries in this lookup definition if you add or modify entries in the License Type field on the target system See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager 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 for Oracle Identity Manager*

Table 1–2 (Cont.) Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Combo.BMC.SupportStaff	You use this lookup definition to specify whether the user is a support staff member.	This lookup definition is preconfigured. You must not modify the entries in this lookup definition.
Combo.BMC.Notify	This lookup definition holds information about the notification mechanism that you can select for a target system account that you create through Oracle Identity Manager. The following is the format of the Code Key and Decode values in this lookup definition: ■ Code Key: Notification mechanism value on the target system ■ Decode: Corresponding notification mechanism value to be displayed in the Notification Method field of the OIM User form	This lookup definition is preconfigured. You can add or modify entries in this lookup definition if you add or modify entries in the Notification Method field on the target system See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager 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 for Oracle Identity Manager*
Combo.BMC.HourlyRate	This lookup definition holds information about the hourly rate currency you can select for a target system account that you create through Oracle Identity Manager. The following is the format of the Code Key and Decode values in this lookup definition: ■ Code Key: Currency value on the target system ■ Decode: Corresponding currency value to be displayed in the Hourly Rate field of the OIM User form	This lookup definition is preconfigured. You can add or modify entries in this lookup definition if you add or modify entries in the Hourly Rate field on the target system See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager 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 for Oracle Identity Manager*

1.7 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 9.1.0.*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 1.7.1, "User Attributes for Target Resource Reconciliation and Provisioning"

- Section 1.7.2, "Support Group Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.7.3, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.7.4, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.7.5, "Provisioning Functions"

1.7.1 User Attributes for Target Resource Reconciliation and Provisioning

Table 1–5 provides information about user attribute mappings for target resource reconciliation and provisioning.

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

Process Form Field	Target System Attribute	Description
User ID	CTM:People.Person ID	User's unique ID
Password	CTM:People.Password	Password
FirstName	CTM:People.First Name	First name of the user
LastName	CTM:People.Last Name	Last name of the user
ClientType	CTM:People.Client Type	Type of user
ProfileStatus	CTM:People.Profile Status	Status of the user profile
ClientSensitivity	CTM:Client Sensitivity	Client sensitivity
VIP	CTM:People.VIP	Specifies whether the user is a very important person
Company+	CTM:People Organization.Company	User's company name
Organization	CTM:People Organization.Organization	Organization to which the user belongs
Department	CTM:People Organization.Department	Department of the user
Site+	SIT:Site Alias Company LookUp.Site	Site to which the user belongs
Region	CTM:Region.Region	Region to which the user belongs The values displayed in this list are specific to the value selected in the Site+ list.
SiteGroup	SIT:Site Group:Site Group	Site group to which the user belongs The values displayed in this list are specific to the value selected in the Region list.
SupportStaff	CTM:People.Support Staff	Specifies whether the user is a support staff
NotificationMethod	CTM:People.Notification Method	Notification method
EmailAddress	CTM:People.Email Address	E-mail address of the user
PrimaryCenterCode	CTM:People.Cost Center Code	Cost center code
HourlyRate	CTM:People.Hourly Rate	Hourly rate
ARLicenseType	CTM:People.License Type	License type
Business Phone	CTM:People.Business	Business phone number
SiteID	CTM:Site ID	Unique site ID

1.7.2 Support Group Attributes for Target Resource Reconciliation and Provisioning

Table 1–4 provides information about support group attribute mappings for target resource reconciliation and provisioning.

Table 1–4 Support Group Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System Support Group Attribute	Description
Support Group Company	CTM:Support Group.Company	Support group company name
Support Group Organization	CTM:Support Group.Organization	Support group organization name
Support Group	CTM:Support Group	Support group name
Support Group Relationship Role	CTM:Support Group. Relationship Role	Support group relationship role name
Support Group ID	Group Id	Support group ID

1.7.3 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 9.1.0.*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: BMC User Recon

Rule element: User Login Equals Users.LoginName

In this rule:

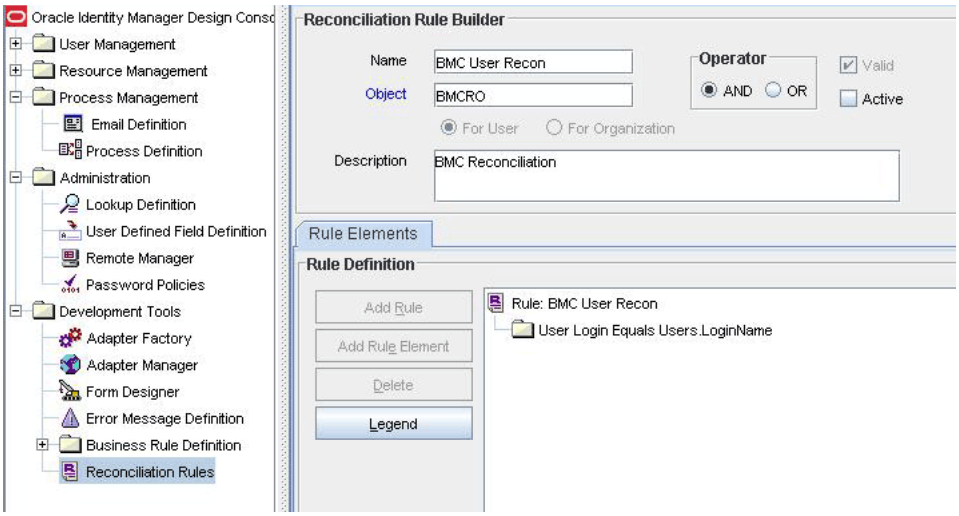
- User Login is the User ID attribute on the OIM User form.
- Users.LoginName is the Login ID attribute of the target system.

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 **BMC User Recon**. Figure 1–2 shows the reconciliation rule for target resource reconciliation.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



1.7.4 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–5 lists the action rules for target resource reconciliation.

Table 1–5 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

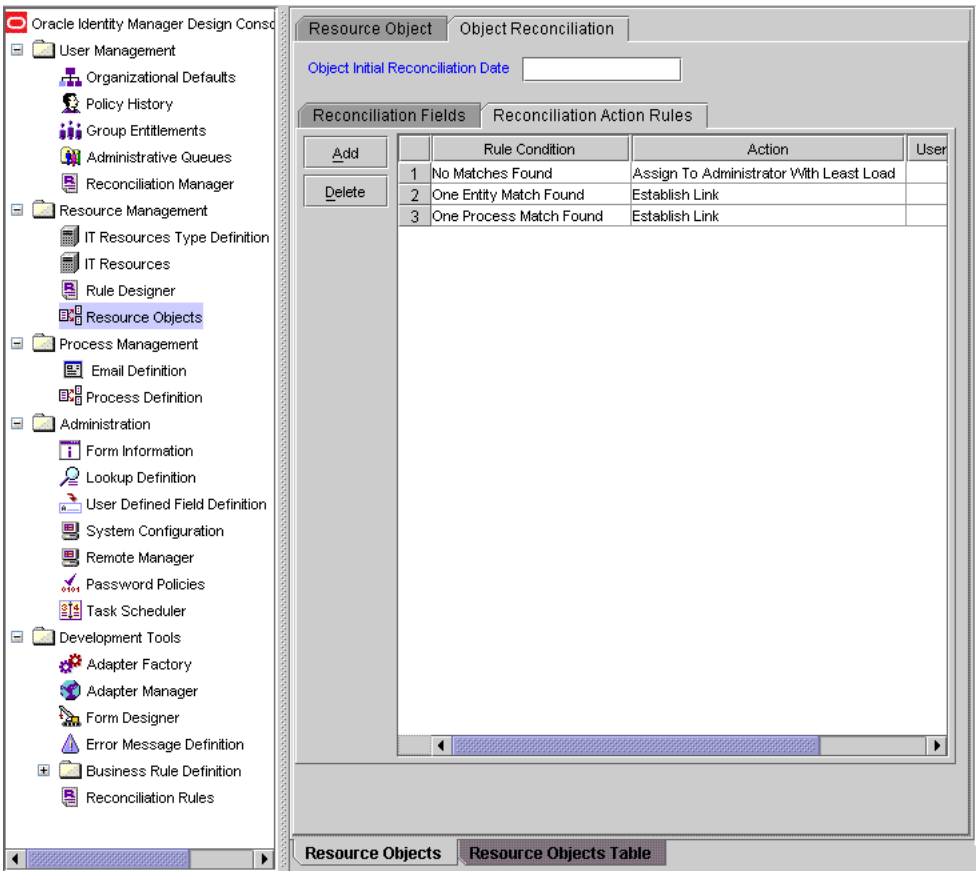
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager 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 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 **BMCRO** 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



1.7.5 Provisioning Functions

Table 1–6 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 1–6 Provisioning Functions

Function	Adapter
Create User	BMCCreateUser
Delete User	BMCDeleteUser
Update User	BMCUpdateUser
Update User Password	BMCUpdateUserPassword
Delete Support Group	BMCDeleteSupportGroup
Update Support Group	BMCupdateSupportGroup

1.8 Connector Objects Used During Trusted Source Reconciliation

The following sections provide information about connector objects used during trusted source reconciliation:

- Section 1.8.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.8.2, "Reconciliation Rule for Trusted Source Reconciliation"

- Section 1.8.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.8.1 User Attributes for Trusted Source Reconciliation

Table 1–7 lists user attributes for trusted source reconciliation.

Table 1–7 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Target System Attribute	Description
User ID	CTM:People.Person ID	User's unique ID
First Name	First Name	First Name
Last Name	Last Name	Last name
Employee Type	NA	Default value: `Consultant`
User Type	NA	Default value: `End-User Administrator`
Organization	NA	Default value: `Xellerate Users`

1.8.2 Reconciliation Rule for Trusted Source Reconciliation

See Also: For generic information about reconciliation matching and action rules, see one of the following guides:

- For Oracle Identity Manager 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: BMCUserTrustedRecon

Rule element: User Login Equals Users.PersonID

In this rule element:

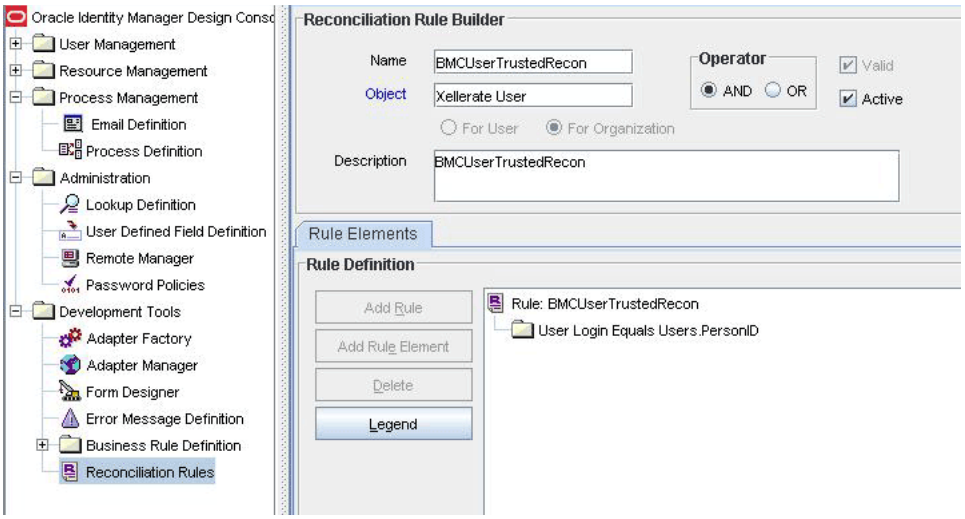
- User Login is the User ID field on the OIM User form.
- Users.PersonID is the CTM:People.Person ID field of BMC Remedy AR System.

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 **BMCUserTrustedRecon.** Figure 1–4 shows the reconciliation rule for trusted source reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



1.8.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–8 lists the action rules for target resource reconciliation.

Table 1–8 Action Rules for Target Source Reconciliation

Rule Condition	Action
No Matches Found	Create User
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

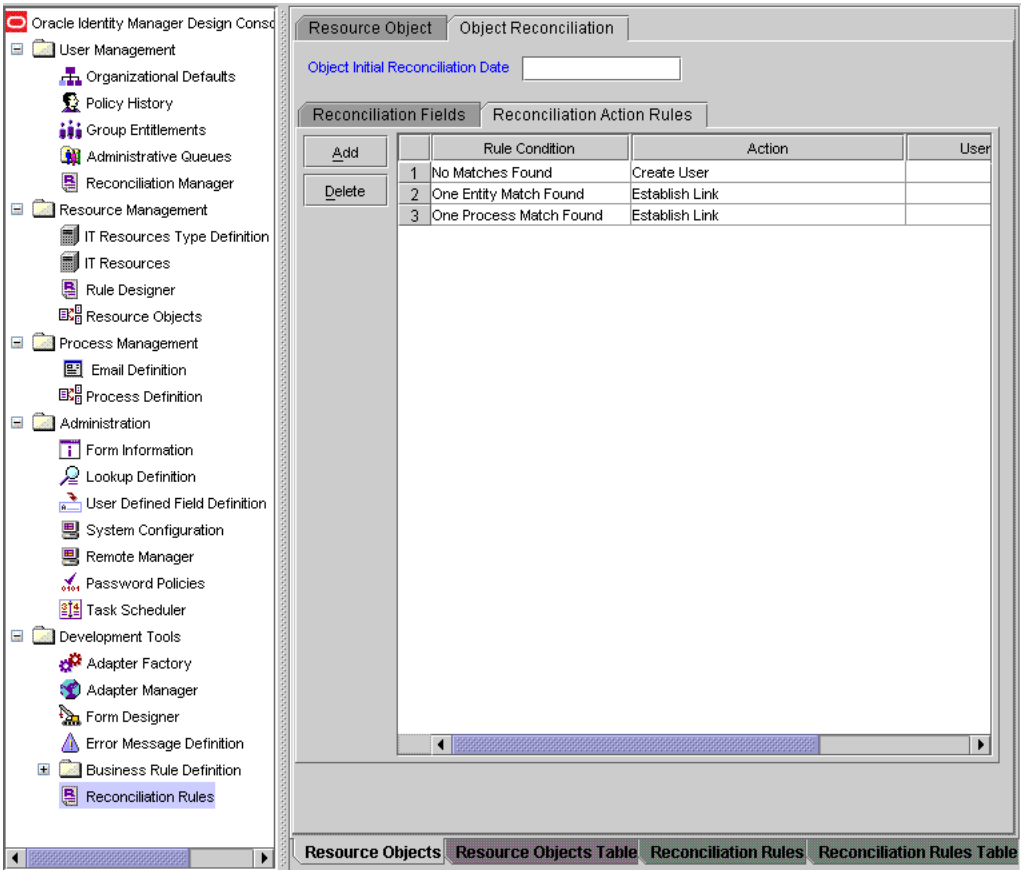
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager 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 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 **Xellerate User** 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 1–5 shows the reconciliation action rules for trusted source reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



1.9 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 guidelines on using the connector and 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"
- Section 2.4, "Installing the Connector on Oracle Identity Manager"
- Section 2.5, "Configuring the Target System"
- Section 2.6, "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 RemedyUser 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/xlBMCRemedy.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 9.1.0.*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
Files 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 9.1.0.*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 and perform provisioning on the target system.
test/config/log.properties	This file is used to store log information.
test/scripts/BMCRemedy.bat test/scripts/BMCRemedy.sh	This file is used to run the test utility.
xml/BMCConnector_DM.xml	This file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Resource object ■ Process form ■ Process definition ■ Process tasks ■ Adapter tasks ■ Lookup definitions ■ Scheduled tasks **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.
xml/BMCXellerateUser_DM.xml	This XML file contains the configuration for the Xellerate User. You must import this file only if you plan to use the connector for trusted source reconciliation.

2.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager 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 xlBMCRemedy.jar file. This file is in the following directory on the installation media:

   OIM_HOME/xellerate/JavaTasks/xlBMCRemedy.jar

2. Open the Manifest.mf file in a text editor. The Manifest.mf file is one of the files bundled inside the xlBMCRemedy.jar file.

   In the Manifest.mf file, the release number of the connector is displayed as the value of the Version property.

2.3 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. Perform one of the following steps:
   - Copy the following files from the BMC Remedy Admin Client installation directory to the *JAVA_HOME*/jre/lib/ext directory:

     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

The procedure to copy external code files ends here. To install the connector on Oracle Identity Manager, proceed to Section 2.4, "Installing the Connector on Oracle Identity Manager."

- Copy the following files from the BMC Remedy Admin Client installation directory to the *OIM_HOME*/xellerate/ThirdParty directory for Oracle Identity Manager release 9.1.0.*x*, and the *OIM_HOME*/server/ThirdParty directory if you are using Oracle Identity Manager 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. Include the following in the `PATH` environment variable:

   Note: You need not perform this step if you have copied the DLL files in Step 2 to the *JAVA_HOME*/jre/lib/ext directory.

   - For Oracle Identity Manager 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 9.1.0.*x*, and the *OIM_HOME*/server/ThirdParty directory if you are using Oracle Identity Manager 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 9.1.0.*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

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 User 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 User 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 2.6.3, "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/BMC/config	*OIM_HOME*/server/XLIntegrations/BMC/config
Files in the test/config directory	*OIM_HOME*/xellerate/XLIntegrations/BMC/config	*OIM_HOME*/server/XLIntegrations/BMC/config
Files in the test/scripts directory	*OIM_HOME*/xellerate/XLIntegrations/BMC/scripts	*OIM_HOME*/server/XLIntegrations/BMC/scripts

2.4.3 Configuring the IT Resource

You must specify values for the parameters of the BMC 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 `BMC` 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
ServerName	IP address or computer name of the BMC Remedy User Management server
Port	TCP/IP port at which the BMC Remedy User Management server is listening The default value is `0`.
TrustedField	Unique identification key for searching user records The default value is `Person ID`.
TrustedTimeStamp	This parameter is used for trusted source reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is `None`. Do not change it.
NonTrustedTimeStamp	This parameter is used for target resource reconciliation. Starting with the first reconciliation run, this parameter stores the time-stamp value at which the reconciliation run ends. The default value is `None`. Do not change it.
IsSecure	Specifies whether or not the encryption feature is enabled The value can be `YES` or `NO`. The default value is `NO`.
DeleteUserFormName	Name of the form in the target system from which details of deleted users can be obtained The value is `CTM:People`.
FormName	Name of the form in the target system from which details of newly created and updated users can be obtained The value is `CTM:People`.

Parameter	Description
NumberOfTrials	Number of times the connection to the target system must be retried before the `InvocationTargetException` is thrown Default value: 2
DelayBetweenTrials	Time difference between subsequent retries (in milliseconds) Default value: 20000
SupportGroupFormName	Name of the form on the target system from which details of newly created and updated support group for a user can be obtained The value is `CTM:Support Group Association`.
SupportGroupTrustedField	Unique identification key for searching support group records for a user. The default value is Support Group Association ID.

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

2.5 Configuring the Target System

Configuring the target system involves the following steps:

- Section 2.5.1, "Enabling Encryption"

2.5.1 Enabling Encryption

This section discusses the following topics related to Remedy encryption:

- Section 2.5.1.1, "Configuring Remedy Encryption"
- Section 2.5.1.2, "AR System Encryption Error Messages"

2.5.1.1 Configuring Remedy Encryption

To enable encryption and set encryption options, you must include server encryption options in the ar.conf file (UNIX) or the ar.cfg file (Microsoft Windows). You can do this by using a text editor.

You can set the `Encrypt-Security-Policy` encryption option. This is an integer value that indicates whether or not encryption is enabled. If this option is not in the ar.cfg (or ar.conf) file, then encryption is disabled by default. If encryption is enabled, then you can set encryption to any one of the following values to this option:

- **0:** Encryption is allowed. Clients and servers with or without encryption enabled on them can connect to this AR System server.
- **1:** Encryption is required. Only clients and servers that have encryption enabled on them can connect to this AR System server.
- **2:** Encryption is disallowed. Regardless of whether or not encryption is enabled, clients and servers can communicate without encryption.

The following table explains sample settings for the options that you can add in the ar.conf (or ar.cfg) file.

Option Settings	Significance
Encrypt-Security-Policy: 1	Encryption is required.

Option Settings	Significance
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.

2.5.1.2 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.
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.

Error Number	Error Message and Description
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.

2.6 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

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

- Section 2.6.2, "Changing to the Required Input Locale"
- Section 2.6.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.6.4, "Enabling Logging"
- Section 2.6.5, "Configuring Oracle Identity Manager for Request-Based Provisioning"

2.6.1 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or a target resource. If you designate the target system as a **trusted source**, then both newly created and modified user accounts are reconciled in Oracle Identity Manager. If you designate the target system as a **target resource**, then only modified user accounts are reconciled in Oracle Identity Manager.

Note: You can skip this section if you do not want to designate the target system as a trusted source for reconciliation.

Configuring trusted source reconciliation involves the following steps:

1. Import the XML file for trusted source reconciliation, BMCXellerateUser_DM.xml, by using the Deployment Manager. This section describes the procedure to import the XML file.

Note: Only one target system can be designated as a trusted source. If you import the BMCXellerateUser_DM.xml file while you have another trusted source configured, then both connector reconciliations would stop working.

2. Specify values for the attributes of the BMC Trusted User Reconciliation scheduled task. This procedure is described later in this guide.

To configure trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. If you are using Oracle Identity Manager release 9.1.0.*x*, then:
   a. Click the **Deployment Management** link on the left navigation bar.
   b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
3. If you are using Oracle Identity Manager release 11.1.1, then:
   a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
4. Locate and open the BMCXellerateUser_DM.xml file, which is in the installation media. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

2.6.2 Changing to the Required Input Locale

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

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

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

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 9.1.0.*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 9.1.0.*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 9.1.0.*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 9.1.0.*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.

2.6.4 Enabling Logging

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

- Section 2.6.4.1, "Enabling Logging on Oracle Identity Manager or Release 9.1.0.x"
- Section 2.6.4.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"

2.6.4.1 Enabling Logging on Oracle Identity Manager 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 messages that highlight the progress of the application at a 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 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.BMCRemedy=log_level
     ```

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

     For example:

     ```
     log4j.logger.Adapter.BMCRemedy=INFO
     ```

  After you enable logging, log information is written to the following file:

  ```
  WebSphere_home/AppServer/logs/server_name/startServer.log
  ```

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, locate the following lines:

     ```
     <category name="Adapter.BMCRemedy">
        <priority value="log_level"/>
     </category>
     ```

  2. In the second XML code line, replace *log_level* with the log level that you want to set. For example:

     ```
     <category name="Adapter.BMCRemedy">
        <priority value="INFO"/>
     </category>
     ```

  After you enable logging, log information is written to the following file:

  ```
  JBoss_home/server/default/log/server.log
  ```

- **Oracle Application Server**

  To enable logging:

  1. Add the following line in the *OIM_HOME*/xellerate/config/log.properties file:

     ```
     log4j.logger.Adapter.BMCRemedy=log_level
     ```

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

     For example:

     ```
     log4j.logger.Adapter.BMCRemedy=INFO
     ```

  After you enable logging, log information is written to the following file:

  ```
  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.BMCRemedy=log_level
   ```

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

   For example:

   ```
   log4j.logger.Adapter.BMCRemedy=INFO
   ```

After you enable logging, log information is written to the following file:

WebLogic_home/user_projects/domains/*domain_name*/*server_name*/*server_name*.log

2.6.4.2 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

Table 2–3 (Cont.) Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
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='bmcremedy-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.BMCREMEDY" level="[LOG_LEVEL]"
useParentHandlers="false">
     <handler name="bmcremedy-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='bmcremedy-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\oim_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.BMCREMEDY" level="NOTIFICATION:1"
useParentHandlers="false">
        <handler name="bmcremedy-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.

2.6.5 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 creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource 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 (account) on the target system.

  Note: Direct provisioning allows the provisioning of multiple target system accounts 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 2.6.5.1, "Copying Predefined Request Datasets"
- Section 2.6.5.2, "Importing Request Datasets into MDS"
- Section 2.6.5.3, "Enabling the Auto Save Form Feature"
- Section 2.6.5.4, "Running the PurgeCache Utility"

2.6.5.1 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_bmcro.xml
- modifyprovisionedresource_bmcro.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\BMCUM

> **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.

2.6.5.2 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 2.6.5.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\BMCUM 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.

2.6.5.3 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 **BMCPROCESS** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.6.5.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.6.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

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:** These sections provide both conceptual and procedural information about configuring the connector. It is recommended that you read the conceptual information before you perform the procedures.

- 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 the Reconciliation 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 user records from the target system are brought into Oracle Identity Manager.

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

> **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 tasks provided for this operation.

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

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

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

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

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

After first-time reconciliation, depending on the mode in which you configure the connector, one of the following parameters of the BMC IT resource is automatically set to the time stamp at which the reconciliation run began:

- For trusted source reconciliation, the TrustedTimeStamp parameter is set.
- For target resource reconciliation, the NonTrustedTimeStamp parameter is set.

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 user records that are added or modified 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 user reconciliation scheduled task.

3.2 Scheduled Task for Lookup Field Synchronization

The BMC 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 the Reconciliation 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
ServerName	Enter the name of the target system IT resource. Default value: `BMC`
TargetRO	This attribute holds the name of the resource object against which lookup field synchronization reconciliation runs must be performed. Value: `BMCRO` **Note:** For the resource object shipped with this connector, you must not change the value of this attribute. However, if you create a copy of the resource object, then you must enter the unique name of that resource object as the value of this attribute.

Table 3–1 (Cont.) Attributes of the Scheduled Task for Lookup Field Synchronization

Attribute	Description
LookUpCodeKey	Enter the name of the lookup field whose values have to be synchronized with the corresponding lookup definitions in Oracle Identity Manager. You can enter one of the following values: ■ Region ■ Site ■ Department ■ Organization ■ SiteGroup ■ SiteID ■ SupportGroupCompany ■ SupportGroupOrganization ■ SupportGroupName ■ RelationshipRole ■ SupportGroupID ■ PrimaryCenterCode Default value: `SupportGroupID`
LookUpFieldCode	Enter the name of the lookup definition corresponding to the lookup field name that you specify in LookUpCodeKey attribute. You can enter one of the following values: ■ Lookup.BMC.Region ■ Lookup.BMC.Site ■ Lookup.BMC.Department ■ Lookup.BMC.Company ■ Lookup.BMC.Organization ■ Lookup.BMC.SiteGroup ■ Lookup.BMC.SiteID ■ Lookup.BMC.SupportCompany ■ Lookup.BMC.SupportOrganization ■ Lookup.BMC.SupportGroup ■ Lookup.BMC.RelationshipRole ■ Lookup.BMC.SupportGroupID ■ Lookup.BMC.PrimaryCentercode ■ Lookup.BMC.PagerSw For example, if you enter `SupportGroupID` as the LookUpCodeKey value, then you must enter `Lookup.BMC.SupportGroupID` as the LookUpFieldCode value. Default value: `Lookup.BMC.SupportGroupID`

Table 3–1 (Cont.) Attributes of the Scheduled Task for Lookup Field Synchronization

Attribute	Description
LookupFormName	Enter the form name on the target system corresponding to the lookup field name that you specify in LookUpCodeKey attribute. You can enter one of the following values: ■ CTM:Region ■ SIT:Site Alias Company LookUp ■ CTM:People Organization ■ CTM:People Organization ■ CTM:People Organization ■ SIT:Site Group ■ SIT:Site ■ CTM:Support Group ■ CTM:Support Group ■ CTM:Support Group ■ SYS:Menu Items For example, if you enter `SupportGroupID` as the LookUpCodeKey value, then you must enter `CTM:Support Group` as the LookupFormName value. Default value: `CTM:Support Group`

3.3 Configuring Reconciliation

As mentioned earlier in this guide, reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts 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 Tasks"

3.3.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records 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 records are reconciled in Oracle Identity Manager.

To perform a full reconciliation run:

- Ensure that the TrustedTimeStamp and NonTrustedTimeStamp parameters of the BMC IT resource are set to `None`.
- Specify `All` as the value of the NumberOfBatches attribute of the user 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 records 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 records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

Creating a filter involves specifying a value for a target system attribute, which will be used in the query SELECT criteria to retrieve the records to be reconciled. You can specify values for any one or a combination of the following target system attributes:

- First Name
- Last Name
- Status
- Notification Method

If you want to use multiple target system attributes to filter records, then you must also specify the logical operator (AND or OR) that you want to apply to the combination of target system attributes that you select.

For example, suppose you specify the following values for these attributes:

- First Name: `John`
- Last Name: `Doe`
- Status: `1`
- Notification Method: `1`
- Operator: `OR`

Because you are using the `OR` operator, during reconciliation, only user records for which *any one* of these criteria is met are reconciled. If you were to use the `AND` operator, then only user records for which *all* of these criteria are met are reconciled.

See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about the scheduled tasks attributes and the logical operator that you want to apply.

Adding New Filter Attributes

If you want to add a filter attribute to the predefined list of filter attributes, then:

1. Add the filter attribute in the scheduled task or the IT resource.

   For example, if you want to add the Middle Name attribute as a filter attribute, then add Middle Name either as a scheduled task attribute or an IT resource parameter. See one of the following guides for information about adding attributes in scheduled tasks and parameters in IT resources:

   - For Oracle Identity Manager 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

2. Depending on whether you are adding a filter attribute for user or group reconciliation, create an entry in one of the following lookup definitions:

   - **For a user attribute**

Create an entry in the Lookup.BMC.UM.QueryAttribute lookup definition. Use the following format to create the entry:

– Code Key: Enter the name of the scheduled task attribute or IT resource parameter that you create in the preceding step.

– Decode: Enter a value in the following format:

CONNECTOR_OBJECT_TYPE,*TARGET_SYSTEM_COLUMN_NAME*,*DATA_TYPE*

In this format:

- *CONNECTOR_OBJECT_TYPE* can be either `ScheduledTask` or `ITResource` depending on whether you add the filter attribute as an attribute of the scheduled task or as a parameter of the IT resource.

- *TARGET_SYSTEM_COLUMN_NAME* is the name of the target system column corresponding to the filter attribute.

- *DATA_TYPE* is the data type of the target system column. It is optional to enter the data type.

The following table shows the default entries in the Lookup.BMC.UM.QueryAttribute lookup definition:

Note: In these default Decode values, `Status, Default Notify Mechanism, First Name, Last Name,` and `Last Modified Date` are the names of target system columns. If the name of any of these columns is different on your target system installation, then replace the column name in the Decode value with the actual name of the target system column. For example, if the name of the Default Notify Mechanism column is `Notify Mechanism 1` on your target system installation, then use the following as the Decode value:

```
ScheduledTask,Notify Mechanism 1
```

Code Key	Decode
Status	ScheduledTask,Status,number
Notification Method	ScheduledTask,Default Notify Mechanism
First Name	ScheduledTask,First Name
Last Name	ScheduledTask,Last Name
NonTrustedTimeStamp	ITResource,Last Modified Date,Date
TrustedTimeStamp	ITResource,Last Modified Date,Date

- **For a group attribute**

  Create an entry in the Lookup.BMC.UM.Grp.QueryAttribute lookup definition. The format of the entry is the same as the format for the Lookup.BMC.UM.QueryAttribute lookup definition described earlier. The following table shows the default entries in the Lookup.BMC.UM.Grp.QueryAttribute lookup definition:

Note: As mentioned in the preceding Note, modify the Decode value so that the column name is the same as the actual column name on your target system installation.

Code Key	Decode
Status	ScheduledTask,Status
NonTrustedTimeStamp	ITResource,Last Modified Date,Date
TrustedTimeStamp	ITResource,Last Modified Date,Date

3. Specify a value for the scheduled task attribute or the IT resource parameter that you create in Step 1. See one of the following sections for information about the procedure:
   - Section 2.4.3, "Configuring the IT Resource"
   - Section 3.3.4, "Reconciliation Scheduled Tasks"

3.3.3 Batched Reconciliation

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

You can configure batched reconciliation to avoid these problems.

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

- BatchSize: Use this attribute to specify the number of records that must be included in each batch. The default value is 1000.
- NumberOfBatches: Use this attribute to specify the total number of batches that must be reconciled. The default value is `All`.

If you specify a value other than `All`, then some of the newly added or modified user records may not get reconciled during the current reconciliation run. The following example illustrates this:

Suppose you specify the following values while configuring the scheduled tasks:

- BatchSize: `20`
- NumberOfBatches: `10`

Suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 200 records would be reconciled during the current reconciliation run. The remaining 114 records would be reconciled during the next reconciliation run.

You specify values for the BatchSize and NumberOfBatches attributes by following the instructions described in Section 3.3.4, "Reconciliation Scheduled Tasks."

3.3.4 Reconciliation Scheduled Tasks

When you run the Connector Installer or import the connector XML file, the following reconciliation scheduled tasks are automatically created in Oracle Identity Manager:

- BMC Trusted User Reconciliation

  This scheduled task is used to reconcile user data in the trusted source (identity management) mode of the connector.

- BMC Non Trusted User Reconciliation

  This scheduled task is used to reconcile user data in the target resource (account management) mode of the connector.

You must specify values for the attributes of these scheduled tasks. Table 3–2 describes the attributes of both scheduled tasks. See Section 3.4, "Configuring the Reconciliation 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.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value were left empty, then reconciliation would not be performed.

Table 3–2 Attributes of the User Reconciliation Scheduled Tasks

Attribute	Description
ServerName	Enter the name of the IT resource for the target system installation from which you want to reconcile user records Default value: `BMC`
IsTrusted	A value of `Yes` implies that you want to configure the connector for trusted source reconciliation. A value of `No` implies that you want to configure the connector for target resource reconciliation. The default value of this attribute in the BMC Non Trusted User Reconciliation scheduled task is `No`. The default value of this attribute in the BMC Trusted User Reconciliation scheduled task is `Yes`. **Note:** It is recommended that you do not change the value of this attribute.
Target RO	Enter the name of the resource object against which reconciliation runs must be performed. Default value: `BMCRO`
XellerateOrganisation	Enter the name of the Oracle Identity Manager organization in which users reconciled from the target system must be created. Default value: `Xellerate Users` **Note:** This attribute is specific to the scheduled task for trusted source reconciliation.
BatchSize	Enter the number of records that must be included in each batch fetched from the target system. If you do not want to implement batched reconciliation, then specify `nodata`. Default value: `1000` **See Also:** Section 3.3.3, "Batched Reconciliation"

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Tasks

Attribute	Description
NoOfBatches	This attribute specifies the number of batches to be reconciled. Enter `All` if you want to reconcile all the batches. This is the default value. Enter an integer value if you want to reconcile only a fixed number of batches. Default value: `All` Sample value: `50` The number of records in each batch is specified by the BatchSize attribute. **See Also:** Section 3.3.3, "Batched Reconciliation"
First Name	This is a filter attribute. Use this attribute to specify the first name of the user whose records you want to reconcile. If you do not want to use this filter attribute, then specify `Nodata`. Default value: `Nodata` **See Also:** Section 3.3.2, "Limited Reconciliation"
Last Name	This is a filter attribute. Use this attribute to specify the last name of the user whose records you want to reconcile. If you do not want to use this filter attribute, then specify `Nodata`. Default value: `Nodata` **See Also:** Section 3.3.2, "Limited Reconciliation"
Notification Method	This is a filter attribute. Use this attribute to specify the notification method for which you want to reconcile user records. The notification method value can be one of the following numbers: ■ 0 (None) ■ 1 (Alert) ■ 2 (Email) ■ 3 (User Default) If you do not want to use this filter attribute, then specify `Nodata`. Default value: `Nodata` **See Also:** Section 3.3.2, "Limited Reconciliation"
Status	This is a filter attribute. Use this attribute to specify the user status for which you want to reconcile user records. The status can be one of the following numbers: ■ 0 (Proposed) ■ 1 (Enabled) ■ 2 (Offline) ■ 3 (Obsolete) ■ 4 (Archive) ■ 5 (Delete) If you do not want to use this filter attribute, then specify `Nodata`. Default value: `Nodata` **See Also:** Section 3.3.2, "Limited Reconciliation"

Table 3–2 (Cont.) Attributes of the User Reconciliation Scheduled Tasks

Attribute	Description
Operator	This is a filter attribute. Enter one of the following values to specify the logical operator to be applied to the filter attribute: ■ AND ■ OR If you do not want to use this filter attribute, then specify `Nodata`. Default value: `Nodata` **See Also:** Section 3.3.2, "Limited Reconciliation"
DateFormat	Enter 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. Default value: `MM/dd/yyyy hh:mm:ss`
QueryAttribute	Enter the name of the lookup definition that stores details of the query attributes. The default value is `Lookup.BMC.UM.QueryAttribute` **See Also:** Section 3.3.2, "Limited Reconciliation"

3.4 Configuring the Reconciliation 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
BMC Lookup Reconciliation	This scheduled task is used to synchronize the values of 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.
BMC Trusted User Reconciliation	This scheduled task is used for reconciling user data when the target system is configured as a trusted source. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.
BMC Non Trusted User Reconciliation	This scheduled task is used for reconciling user data when the target system is configured as a target resource. See Section 3.3.4, "Reconciliation Scheduled Tasks" for information about this scheduled task.

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.
- Attributes of the scheduled task are discussed in the following sections:

  Section 3.2, "Scheduled Task for Lookup Field Synchronization"

  Section 3.3.4, "Reconciliation Scheduled Tasks"

- 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 target system account 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: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

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 target system account, then:
   - If you are using Oracle Identity Manager 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 target system account to an existing OIM User, then:
   - If you are using Oracle Identity Manager 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 9.1.0.*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 **BMCRO** 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 User page, enter the details of the account that you want to create on the target system and then click **Continue**.
8. On the Step 5: Provide Process Data for BMC Update Support Groups and Roles page, if required, enter details of the support groups and roles and then click **Continue**.
9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
10. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
    - If you are using Oracle Identity Manager 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 target system account. 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, 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 account..

   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 **BMCRO**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account 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 2.6.5, "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 **BMCPROCESS** 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 **BMCRO** 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 **BMCPROCESS** 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 **BMCRO** 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:

> **Note:** In the following sections, the term **attribute** refers to the identity data fields that store user data.

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

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.

By default, the attributes listed in Section 1.7, "Connector Objects Used During Target Resource Reconciliation and Provisioning" are mapped for reconciliation between Oracle Identity Manager and the target system. 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 9.1.0.*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 CTM:People form.

e. Double-click the field whose Database ID you want to determine.

f. On the Database tab, the Database ID of the field is displayed as the value of the ID field.

2. Modify the attributemapping_recon.properties file, which is in the *OIM_HOME*/xellerate/XLIntegrations/BMC/config directory.

   At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

   OIM_ATTRIBUTE_NAME=DATABASE_ID_IN_BMC_REMEDY

   For example:

   `Users.EmailAddress=260000002`

   In this example, `EmailAddress` is the reconciliation field and 260000002 is the equivalent Database ID in BMC Remedy System. As a standard, the prefix "`Users.`" is added at the start of all reconciliation field names.

3. In the resource object definition, add a reconciliation field corresponding to the new attribute as follows:

   a. Open the Resource Objects form. This form is in the Resource Management folder.

   b. Click **Query for Records**.

   c. On the Resource Objects Table tab, double-click the BMCRO resource object to open it for editing.

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

   e. Specify a value for the field name.

      You must specify the name that is to the left of the equal sign in the line that you uncomment or add while performing Step 2.

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

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

      For example: `String`

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

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

   i. 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.

4. Modify the process definition to include the mapping between the newly added attribute and the corresponding reconciliation field as follows:

   a. Open the Process Definition form. This form is in the Process Management folder.

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

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

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

5. 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

By default, the attributes listed in Section 1.7, "Connector Objects Used During Target Resource Reconciliation and Provisioning" are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning as follows:

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

- For Oracle Identity Manager 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 CTM:People form.

   e. Double-click the field whose Database ID you want to determine.

   f. On the Database tab, the Database ID of the field is displayed as the value of the ID field.

2. Modify the attributemapping_prov.properties file, which is in the *OIM_HOME*/xellerate/XLIntegrations/BMC/config directory.

   At the end of this file, some of the attribute definitions are preceded by comment characters. You can uncomment the definition of an attribute to make it a part of the list of reconciliation attributes. If required, you can also add new attributes in this file. The format that you must use is as follows:

   ```
   OIM_ATTRIBUTE_NAME=DATABASE_ID_IN_BMC_REMEDY
   ```

   For example:

   ```
   EmailAddress=260000002
   ```

   In this example, `EmailAddress` is the reconciliation field and `260000002` is the equivalent Database ID in BMC Remedy System.

3. Add a new column in the process form.

   a. Open the process form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

   b. Click **Create New Version**.

c. In the Create a New Version dialog box, specify the version name in the **Label** field, save the changes, and then close the dialog box.

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

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

f. Specify the new field name and other values. For the example described in Step 3 of Section 4.1, "Adding Custom Attributes for Reconciliation," enter `UB_BMC_EMAIL`.

4. Add a new variable in the variable list.

a. Open the Adapter Factory form. This form is in the Development Tools folder of the Oracle Identity Manager Design Console.

b. Click the **Query for Records** icon.

c. On the Adapter Factory Table tab, double-click the **adpBMCCREATEUSER** adapter from the list.

d. On the Variable List tab, click **Add**.

e. In the Add a Variable dialog box, specify the required values and then save and close the dialog box.

5. Define an additional adapter task for the newly added variable in the **adpBMCCREATEUSER** adapter.

a. On the Adapter Tasks tab of the Adapter Factory form, click **Add**.

b. In the Adapter Task Selection dialog box, select **Functional Task**, select **Java** from the list of functional task types, and then click **Continue**.

c. In the Object Instance Selection dialog box, select **Persistent Instance** and then click **Continue**.

d. In the Add an Adapter Factory Task dialog box, specify the task name, select the **setProperty** method from the **Method** list, and then click **Save**.

e. Map the application method parameters, and then save and close the dialog box. To map the application method parameters:

For the "Output: String Return variable (Adapter Variable)" parameter:

i. From the **Map to** list, select **Literal**.

ii. From the **Name** list, select **Return variable**.

For the "Input: String input (Adapter Variable)" parameter:

i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select **Input**.

For the "Input: String Status (Literal)" parameter:

i. From the **Map to** list, select **Literal**.

ii. From the **Name** list, select **String**.

iii. In the **Value** field, enter **Status**.

For the "Input: String Status (Adapter Variable)" parameter:

i. From the **Map to** list, select **Adapter Variables**.

ii. From the **Name** list, select **Status**.

f. Repeat Steps b through g to create more adapter tasks.

6. Create an additional adapter task to set the input variable.
   a. Open the Adapter Factory form. This form is in the Development Tools folder in the Oracle Identity Manager Design Console.
   b. On the Adapter Tasks tab, click **Add**.
   c. In the Adapter Task Selection dialog box, select **Logic Task**, select **SET VARIABLE** from the list, and then click **Continue**.
   d. In the Edit Set Variable Task Parameters dialog box, select **input** from the **Variable Name** list, select **Adapter Task** from the **Operand Type** list, and the Operand Qualifier as the Adapter Task that you have created in the previous step. Then, click **Save**.
7. Map the process form columns and adapter variables for the Create User process task as follows:
   a. Open the Process Definition form. This form is in the Process Management folder of the Design Console.
   b. Click the **Query for Records** icon.
   c. On the Process Definition Table tab, double-click the **BMCPROCESS** process.
   d. On the Tasks tab, double-click the **Create User** task.
   e. In the Closing Form dialog box, click **Yes**.
   f. On the Integration tab of the Editing Task Columns Create User dialog box, map the unmapped variables, and then save and close the dialog box. To map an unmapped variable:

      i. Double-click the row in which **N** is displayed in the Status column. The value `N` signifies that the variable is not mapped.

      ii. From the **Map to** list in the Edit Data Mapping for Variables dialog box, select **Process Data**.

      iii. From the **Qualifier** list, select the name of the variable.

      Repeat Steps i through iii for all unmapped variables.

   Repeat Steps 1 through 6 if you want to add more attributes.
8. Update the request datasets.

   Note: Perform steps 8 through 10 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 3 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_BMC_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 3.
- For the type attribute, enter the value that you entered in the Variant Type column of the process form while performing Step 3.
- For the widget attribute, enter the value that you entered in the Field Type column of the process form, while performing Step 3.
- For the length attribute, enter the value that you entered in the Length column of the process form while performing Step 3.
- 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.

9. 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.

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

See Section 2.6.5.2, "Importing Request Datasets into MDS" for detailed information about the procedure.

11. 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 Installations of the Target System

Note: Perform this procedure only if you want to configure the connector for multiple installations of BMC Remedy User Management.

You may want to configure the connector for multiple installations of BMC Remedy User Management. The following example illustrates this requirement:

The Tokyo, London, and New York offices of Example Multinational Inc. have their own installations of BMC Remedy User Management. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of BMC Remedy User Management.

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of BMC Remedy User Management.

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

See Also: One of the following guides for detailed instructions on performing each step of this procedure:

- For Oracle Identity Manager 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 each target system installation.

   The Resource Objects form is in the Resource Management folder. The BMCRO resource object is created when you import the connector XML file. You can use this resource object as the template for creating the remaining resource objects.

2. Create and configure one IT resource for each resource object.

   The IT Resources form is in the Resource Management folder. The BMCRO IT resource is created when you import the connector XML file. You can use this IT resource as the template for creating the remaining IT resources, of the same resource type.

3. Design one process form for each resource object.

   The Form Designer form is in the Development Tools folder. The UD_BMC process form is created when you import the connector XML file. You can use this process form as the template for creating the remaining process forms.

4. Create and configure one process definition for each resource object.

   The Process Definition form is in the Process Management folder. The BMCPROCESS process definition is created when you import the connector XML file. You can use this process definition as the template for creating the remaining process definitions.

   While creating process definitions for each target system installation, the following steps that you must perform are specific to the creation of each process definition:

   - From the **Object Name** lookup field, select the resource object that you create in Step 1.
   - From the **Table Name** lookup field, select the process form that you create in Step 3.
   - While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.

5. Configure reconciliation for each target system installation. See Section 3.4, "Configuring the Reconciliation Scheduled Tasks" for instructions.

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.

For each target system installation, only the values of the following attributes of the scheduled task must be changed:

- TargetRO
- ServerName
- IsTrusted

Set the IsTrusted attribute to `YES` for the BMC Remedy User Management installation that you want to designate as a trusted source.

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

When you use the Administrative and User Console to perform provisioning, you can specify the IT resource corresponding to the BMC Remedy User Management installation to which you want to provision the user.

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 the following directory:
   - For Oracle Identity Manager release 9.1.0.*x*:

     OIM_HOME/xellerate/XLIntegrations/BMC/test/config
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/XLIntegrations/BMC/test/config

     Note: The parameters in the config.properties file are the same as the IT resource parameters.
2. Run one of the following scripts:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then run the following script:

     For UNIX:

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

     For Microsoft Windows:

     OIM_HOME\xellerate\XLIntegrations\tests\scripts\BMCRemedy.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/BMCRemedy.sh

For Microsoft Windows:

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

5.1.1 Testing Limited and Batched Reconciliation

You can test both limited and batched reconciliation, in either trusted source or target resource mode, by specifying values for the following user reconciliation attributes:

- BatchSize
- NoOfBatches
- First Name
- Last Name
- Notification Method
- Status
- Operator

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

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

- BatchSize: `4`
- NoOfBatches: `2`
- First Name: `John`
- Last Name: `Doe`
- Notification Method: `Nodata`
- Status: `1`
- Operator: `AND`

Suppose you specify these values in the target resource user reconciliation scheduled task. After that task is run, all target system records for which the first name and last name values are `John` and `Doe`, respectively, are divided into batches of four records each. Of these batches, the first two are reconciled during the current reconciliation run.

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 Remedy User Management server is running. ■ Ensure that Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that values for all the IT resource parameters have been correctly specified.

Problem Description	Solution
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: `java.lang.UnsatisfiedLinkErrorwrong ELF data format:ELFDATA2MSB`	Ensure that you are using the specified shared object (.so) files. These files are platform dependent. For example, .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

The following are known issues associated with this release of the connector:

- **Bug 7207232**

  Some Asian languages use multibyte character sets. If the character limit for the fields in the target system is specified in bytes, then the number of Asian-language characters that you can enter in a particular field may be less than the number of English-language characters that you can enter in the same field. The following example illustrates this limitation:

  Suppose you can enter 50 characters of English in the User Last Name field of the target system. If you were using the Japanese language and if the character limit for the target system fields were specified in bytes, then you would not be able to enter more than 25 characters in the same field.

- **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 one of the following guides for more information:

  - For Oracle Identity Manager 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

  When you create entries, you must copy the key for each entry from the resource bundle for English.

- **Bug 8367021**

  The following issue is observed during trusted source reconciliation:

  If a user is marked as Deleted on the target system and if that user has not been reconciled earlier in Oracle Identity Manager, then the user is created in the Enabled state on Oracle Identity Manager at the end of the reconciliation run.

  This problem is automatically resolved at the end of the next reconciliation run. At that time, the status of the user in Oracle Identity Manager is set to Disabled.

Index

A

Administrative and User Console, 2-12, 5-3
architecture of the connector, 1-3

C

certified components, 1-2
changing input locale, 2-11, 2-12
clearing server cache, 2-12
configuring
  connector for multiple installations of the target system, 4-6
  Oracle Identity Manager server, 2-11
  target system, 2-9
configuring connector, 3-1
connector architecture, 1-3
connector configuration, 3-1
connector files and directories
  copying, 2-3
  description, 2-1
  destination directories, 2-3
connector installer, 2-5
connector testing, 5-1
connector version number, determining, 2-2
creating scheduled tasks, 3-11

D

defining
  IT resources, 2-8
  scheduled tasks, 3-11
determining version number of connector, 2-2

E

enabling encryption, 2-9
enabling logging, 2-14
encryption
  enabling, 2-9
  error messages, 2-10
  Remedy, 2-9
errors, 5-2

F

files and directories of the connector
  See connector files and directories

G

globalization features, 1-3

I

input locale changing, 2-11
input locale, changing, 2-12
installing connector, 2-5
IT resources
  BMC, 2-8
  defining, 2-8
  parameters, 2-8

K

known issues, 6-1

L

limitations, 6-1
logging enabling, 2-14
lookup field synchronization, 1-6
lookup fields, 1-6

M

multilanguage support, 1-3

O

Oracle Identity Manager Administrative and User Console, 2-12, 5-3
Oracle Identity Manager server, configuring, 2-11

P

parameters of IT resources, 2-8
problems, 5-2
provisioning, 3-13
  direct provisioning, 3-14
  provisioning triggered by policy changes, 3-14
  request-based provisioning, 3-14
provisioning functions, 1-13

R

reconciliation
module, 1-9
reconciliation rule
target resource reconciliation, 1-11, 1-14
Remedy encryption
configuring, 2-9

S

scheduled tasks
defining, 3-11
server cache, clearing, 2-12
supported
releases of Oracle Identity Manager, 1-2
target systems, 1-2
supported languages, 1-3

T

target resource reconciliation
reconciliation action rules, 1-12, 1-15
reconciliation rule, 1-11, 1-14
target system configuration, 2-9
target system, multiple installations, 4-6
target systems supported, 1-2
testing connector, 5-1
testing the connector, 5-1
testing utility, 5-1
troubleshooting, 5-2

V

version number of connector, determining, 2-2