Oracle® Identity Manager

Connector Guide for BMC Remedy User Management

11.1.1
E40750-10
May 2020

Oracle Identity Manager Connector Guide for BMC Remedy User Management, 11.1.1

E40750-10

Primary Author: Alankrita Prakash

Contributing Authors: Gowri.G.R

Contents

2 Deploying the Connector

3 Using the Connector

List of Figures

List of Tables

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 that have purchased support 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, visit the following Oracle Help Center page: http://docs.oracle.com/cd/E52734_01/index.html

For information about Oracle Identity Manager Connectors documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E22999_01/index.htm

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 Oracle Identity Manager Connector for BMC User Management?

This chapter provides an overview of the updates made to the software and documentation for release 11.1.1.6.0 of the BMC User Management connector.

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

- Software Updates

  This section describes updates made to the connector software. This section also points out the sections of this guide that have been changed in response to each software update.

- Documentation-Specific Updates

  This section describes major changes made to this guide. For example, the relocation of a section from the second chapter to the third chapter is a documentation-specific update. These changes are not related to software updates.

Software Updates

The following sections discuss software updates:

- Software Updates in Release 11.1.1.6.0
- Software Updates in Release 11.1.1.5.0

Software Updates in Release 11.1.1.6.0

The following are the software updates in release 11.1.1.6.0:

- Support for Performing Reconciliation and Provisioning Operations on Custom Forms
- Support for Performing Lookup Field Synchronization Against Custom Forms
- Issues Resolved in Release 11.1.1.6.0

Support for Performing Reconciliation and Provisioning Operations on Custom Forms

By default, this connector provisions to and reconciles data from the CTM:People form. From this release onward, the connector can be configured to perform reconciliation and provisioning operations on custom forms in the target system. See Configuring the Connector for Performing Reconciliation and Provisioning Operations on Custom Forms.

Support for Performing Lookup Field Synchronization Against Custom Forms

The connector performs lookup field synchronization against the default forms (available in the target system) associated with each lookup field. From this release onward, you can specify target system form names against which lookup field synchronization must be performed. See Configuring the Connector for Performing Lookup Field Synchronization on Custom Forms.

Issues Resolved in Release 11.1.1.6.0

The following are issues resolved in release 11.1.1.6.0:

Bug Number	Issue	Resolution
17388344	The following error was encountered when you tried creating a new version of the UD_BMC process form on Oracle Identity Manager release 11.1.1.*x:* `Invalid property name was specified.`	This issue is encountered if the UD_BMC_PWD process form field has the AccountPassword property set to `true`, which is not supported in Oracle Identity Manager release 11.1.1.*x.* This issue has been resolved. **Note:** This issue exists if you are using release 11.1.1.5.0 of this connector with Oracle Identity Manager release 11.1.1.*x.* Therefore, as a workaround, perform the following steps: 1. In Oracle Identity Manager Administration, export the **UD_BMC** connector process form by clicking **Export Deployment Manager File** under System Management. 2. In a text editor, open the exported XML file for editing. 3. Search for and remove a code snippet similar to the following: `<FormFieldProperty repo-type="RDBMS" id="SDP90"> <SDP_PROPERTY_VALUE>true</SDP_PROPERTY_VALUE> <SDP_UPDATE>1360054099000</SDP_UPDATE> <SDP_PROPERTY_NAME>AccountPassword</ SDP_PROPERTY_NAME> </FormFieldProperty>` **Note:** Change the form versions from the existing version to a new version. 4. Save and close the file. 5. Import the modified XML into Oracle Identity Manager by clicking the import deployment manager file link. See *Oracle Fusion Middleware Administering Oracle Identity Manager* for release 11.1.1.*x* for detailed instructions about the procedure.
17388395	When two or more support groups are assigned to a user, the Delete Support Group provisioning operation always removed the support group that was first assigned to the user, irrespective of the support group that was intended to be deleted.	This issue has been resolved.

Software Updates in Release 11.1.1.5.0

The following are the software updates in release 11.1.1.5.0:

- Identity Connector Framework Based Implementation
- Support for New Versions of the Target System
- Dependency on Native Libraries Eliminated
- Support for Oracle Identity Manager 11*g* Release 2 BP04 or Later
- Transformation and Validation of Account Data

Identity Connector Framework Based Implementation

The Identity Connector Framework (ICF) is a component that provides basic provisioning, reconciliation, and other functions that all Oracle Identity Manager and Oracle Waveset connectors require. The ICF also uses classpath isolation, which allows the BMC Remedy User Management connector to co-exist with legacy versions of the connector. See Certified Components.

As this connector is ICF-based:

- you can deploy the connector in a Connector Server. See Deploying the Connector in a Connector Server.
- the connector supports connector pooling. See Connection Pooling.
- separate scheduled jobs for performing lookup field synchronization are available. See Scheduled Job for Lookup Field Synchronization.

Support for New Versions of the Target System

From this release onward, the connector adds support for all target system releases from 7.1 through 8.1.

These target system versions are mentioned in Certified Components.

Dependency on Native Libraries Eliminated

For target system releases prior to the BMC Remedy AR System 7.1, the connector used native APIs to connect to the target system. These native APIs were platform dependent. Therefore, the native libraries from the target system had to be placed in the classpath of Oracle Identity Manager.

From BMC Remedy AR System 7.1 onwards, the target supports the use of pure Java APIs for the connector to establish a connection with the target system. Therefore, this connector (which supports AR System versions 7.1 through 8.1) has no dependency on the native libraries of the target system.

Support for Oracle Identity Manager 11*g* Release 2 BP04 or Later

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) or later. This Oracle Identity Manager version is mentioned in Certified Components.

Transformation and Validation of Account Data

You can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation. In addition, you can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. See the following sections for more information:

- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During Reconciliation

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 11.1.1.6.0
- Documentation-Specific Updates in Release 11.1.1.5.0

Documentation-Specific Updates in Release 11.1.1.6.0

The following is a documentation-specific updates in revision "10" of release 11.1.1.6.0:

The "Oracle Identity Governance or Oracle Identity Manager" row in Table 1-1 has been modified to include support for Oracle Identity Governance release 12*c* PS4 (12.2.1.4.0).

The following are the documentation-specific updates in revision "9" of release 11.1.1.6.0:

- The "Target system" row of Table 1-1 has been updated to include BMC Remedy AR System version 9.1.07.
- Minor updates to the document structure for better readability.

The following is a documentation-specific update in revision "8" of release 11.1.1.6.0:

The "Target system" row of Table 1-1 has been updated to include note that BMC Remedy 9.1 target needs JDK 1.8u45 or later.

The following is a documentation-specific update in revision "7" of release 11.1.1.6.0:

The "Target system" row of Table 1-1 has been updated to include support to BMC Remedy target system 9.1.

The following is a documentation-specific update in revision "6" of release 11.1.1.6.0:

The "JDK" row of Table 1-1 has been renamed to "Connector Server JDK".

The following are documentation-specific updates in revision "5" of release 11.1.1.6.0:

- The "Oracle Identity Manager" row of Table 1-1 has been updated.
- Information specific to Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0) has been added to Usage Recommendation.

The following is a documentation-specific update in revision "4" of release 11.1.1.6.0:

A "Note" regarding lookup queries has been added at the beginning of Extending the Functionality of the Connector.

The following is a documentation-specific update in revision "3" of release 11.1.1.6.0:

Information about limited reconciliation has been modified in Performing Limited Reconciliation.

The following are documentation-specific updates in release 11.1.1.6.0:

- An example has been added in Step 1 of Copying the External Code Files.
- Configuring the Password Form Field has been added.

Documentation-Specific Updates in Release 11.1.1.5.0

There are no documentation-specific updates in this release.

1

About the Connector

This chapter introduces the BMC Remedy User Management 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.

> **Note:**
>
> 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.

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.

> **Note:**
>
> It is recommended that you do not configure the target system as both an authoritative (trusted) source and a managed (target) resource.

This chapter contains the following sections:

1.1 Certified Components

These are the software components and their versions required for installing and using the BMC Remedy User Management connector.

Table 1-1 lists the certified components for all target systems.

Table 1-1 Certified Components

Item	Requirement
Oracle Identity Governance or Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: • Oracle Identity Governance release 12*c* (12.2.1.4.0) • Oracle Identity Governance release 12*c* (12.2.1.3.0) • Oracle Identity Manager 11*g* Release 1 PS1 BP07 (11.1.1.5.7) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 BP04 (11.1.2.0.4) and any later BP in this release track • Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0)
Target system	The target system can be any one of the following: • BMC Remedy AR System 7.1 through 9.1 • BMC Remedy AR System 9.1.07 **Note:** The target system does not support SSL communication. Remedy 9.1 target needs JDK 1.8u45 or later.
Connector Server	11.1.2.0.0
Connector Server JDK	JDK 1.6 update 24 or later, or JRockit JDK 1.6 update 17 or later

1.2 Usage Recommendation

These are the recommendations for the connector versions that you can deploy and use depending on the Oracle Identity Manager version that you are using.

- If you are using a release that is earlier than Oracle Identity Manager 11*g* Release 1 (11.1.1) (for example, Oracle Identity Manager 9.0.1 through 9.0.3.*x* or release 9.1.0.1), then you must use the 9.0.4.*x* version of this connector.
- If you are using Oracle Identity Manager 11*g* Release 1 (11.1.1.5.7) or later, Oracle Identity Manager 11*g* Release 2 (11.1.2.0.4) or later, or Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0), 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

These are the languages that the connector supports.

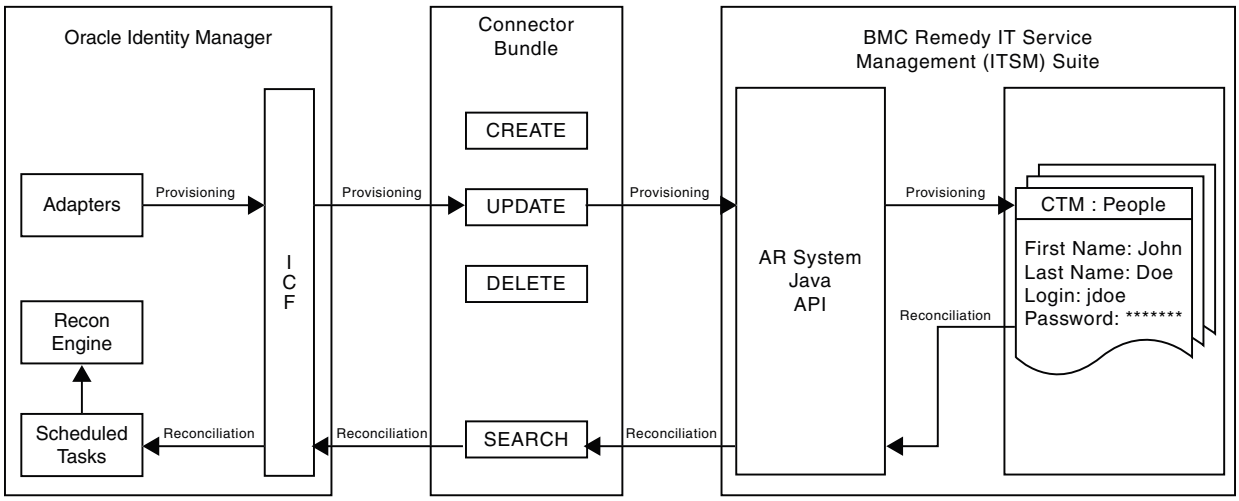
- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Czech
- Danish
- Dutch
- English (US)
- Finnish
- French
- German
- Greek
- Hebrew
- Hungarian
- Italian
- Japanese
- Korean
- Norwegian
- Polish
- Portuguese
- Portuguese (Brazilian)
- Romanian
- Russian
- Slovak
- Spanish
- Swedish
- Thai
- Turkish

1.4 Connector Architecture

You can configure the BMC Remedy User Management connector to either run the Identity Reconciliation mode or Account Management mode. This connector is implemented using the Integrated Common Framework (ICF) component.

Figure 1-1 shows the architecture of the connector.

Figure 1-1 Connector Architecture



The BMC Remedy User Management connector is implemented by using the Identity Connector Framework (ICF). The ICF is a component that provides basic reconciliation and provisioning operations that are common to all Oracle Identity Manager connectors. In addition, ICF provides common features that developers would otherwise need to implement on their own, such as connection pooling, buffering, time outs, and filtering. The ICF is shipped along with Oracle Identity Manager. Therefore, you need not configure or modify the ICF.

The primary function of this connector is to create Users in the BMC Remedy IT Service Management (ITSM) application through Oracle Identity Manager. The BMC Remedy ITSM Suite consists of a core system called the Action Request System (AR System). This connector integrates Oracle Identity Manager with the BMC Remedy System (target system) with the help of a Java API that is exposed by the AR System.

The target system can be configured to run in one of the following modes:

- Identity reconciliation

  Identity reconciliation is also known as authoritative or trusted source reconciliation. In this mode, the target 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 jobs) about these target system users into Oracle Identity Manager. This data is used to create or update the corresponding OIM Users.

- Account Management

  Account management is also known as target resource management. In this mode, the target system is used as a target resource and the connector enables the following operations:

  – Provisioning

    Provisioning involves creating, updating, or deleting users on the target system through Oracle Identity Manager. Users are created during provisioning in the People form of the target system. The connector makes use of the Java API to connect to the Remedy Server, and in turn provision the account.

– Target resource reconciliation

  During reconciliation, the user management connector fetches data (using scheduled jobs) 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.

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

For provisioning operations such as Create, Update, and Delete, and reconciliation operations such as Search, Oracle Identity Manager makes SPI calls to ICF, which triggers corresponding operations on the connector bundle. The connector bundle invokes the AR System API to connect to the target system by using information about the BMC Remedy server name, AR System user and password from the IT resource.

During reconciliation, a schedule task is run which calls the SearchOp operation of the connector bundle. Like provisioning, the connector invokes the AR System API to get the list of entries from the respective form (for Users or Lookup) by passing the batching and filter parameters. This result is then passed to Oracle Identity Manager.

1.5 Features of the Connector

The features of the connector include support for full and incremental reconciliation, limited reconciliation, batched reconciliation, transformation and validation of account data and so on.

This connector supports the following features:

- Support for Both Target Resource and Trusted Source Reconciliation
- Full and Incremental Reconciliation
- Limited Reconciliation
- Batched Reconciliation
- Reconciliation of Deleted User Records
- Transformation and Validation of Account Data
- Support for Connector Server
- Connection Pooling

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 Configuring Reconciliation.

1.5.2 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. In incremental

reconciliation, user accounts that have been added or modified since the last reconciliation run are fetched into Oracle Identity Manager.

You can perform a full reconciliation run at any time as described in Performing Full Reconciliation.

1.5.3 Limited Reconciliation

You can set a reconciliation filter as the value of the Filter attribute of the user reconciliation scheduled job. This filter specifies the subset of added and modified target system records that must be reconciled.

See Performing Limited Reconciliation.

1.5.4 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 Performing Batched Reconciliation.

1.5.5 Reconciliation of Deleted User Records

You can configure the connector for reconciliation of deleted user records. In target resource mode, if a user record is deleted on the target system, then the corresponding BMC user resource is revoked from the OIM User. In trusted source mode, if a user record is deleted on the target system, then the corresponding OIM User is deleted.

See Scheduled Job for Reconciliation of Deleted Users Records for more information about scheduled jobs used for reconciling deleted user records

1.5.6 Transformation and Validation of Account Data

You can configure validation of account data that is brought into or sent from Oracle Identity Manager during reconciliation and provisioning. In addition, you can configure transformation of account data that is brought into Oracle Identity Manager during reconciliation.

The following sections provide more information:

- Configuring Validation of Data During Reconciliation and Provisioning
- Configuring Transformation of Data During Reconciliation

1.5.7 Support for Connector Server

Connector Server is a component provided by ICF. By using one or more connector servers, the connector architecture permits your application to communicate with externally deployed bundles. In other words, a connector server enables remote execution of an Oracle Identity Manager connector.

A Java connector server is useful when you do not wish to execute a Java connector bundle in the same VM as your application. It can be beneficial to run a Java connector on a different host for performance improvements.

See Deploying the Connector in a Connector Server.

1.5.8 Connection Pooling

A connection pool is a cache of objects that represent physical connections to the target. Oracle Identity Manager connectors can use these connections to communicate with target systems. At run time, the application requests a connection from the pool. If a connection is available, then the connector uses it and then returns it to the pool. A connection returned to the pool can again be requested for and used by the connector for another operation. By enabling the reuse of connections, the connection pool helps reduce connection creation overheads like network latency, memory allocation, and authentication.

One connection pool is created for each IT resource. For example, if you have three IT resources for three installations of the target system, then three connection pools will be created, one for each target system installation.

See Setting up the Lookup Definition for Connection Pooling.

1.6 Lookup Definitions Used During Reconciliation and Provisioning

Lookup definitions used during reconciliation and provisioning can be divided into the following categories:

- Lookup Definitions Synchronized with the Target System
- Preconfigured Lookup Definitions

1.6.1 Lookup Definitions Synchronized with the Target System

Lookup field synchronization involves copying additions or changes made to the target system lookup fields into the lookup definitions in Oracle Identity Manager.

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 Organizational Unit lookup field to select an organizational unit from the list of organizational units in the lookup field. When you deploy the connector, lookup definitions corresponding to the lookup fields on the target system are created in Oracle Identity Manager.

The following lookup definitions are populated with values fetched from the target system by the scheduled jobs for lookup field synchronization:

- Lookup.BMC.Company
- Lookup.BMC.Department
- Lookup.BMC.Organization
- Lookup.BMC.PrimaryCenterCode
- Lookup.BMC.Region
- Lookup.BMC.Site
- Lookup.BMC.SiteGroup
- Lookup.BMC.SiteID

- Lookup.BMC.SupportGroupID

1.6.2 Preconfigured Lookup Definitions

This section discusses 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.

The other lookup definitions are as follows:

- Lookup.BMC.Configuration
- Lookup.BMC.Configuration.Trusted
- Lookup.BMC.UM.Configuration
- Lookup.BMC.UM.Configuration.Trusted
- Lookup.BMC.UM.ProvAttrMap
- Lookup.BMC.UM.ReconAttrMap
- Lookup.BMC.UM.ReconAttrMap.Trusted
- Lookup.BMC.UM.ReconDefaults.Trusted
- Lookup.BMC.ARLicenseType
- Lookup.BMC.ClientType
- Lookup.BMC.SupportStaff
- Lookup.BMC.VIP
- Lookup.BMC.ClientSensitivity
- Lookup.BMC.ProfileStatus
- Lookup.BMC.HourlyRate

1.6.2.1 Lookup.BMC.Configuration

The Lookup.BMC.Configuration lookup definition holds connector configuration entries that are used during target resource reconciliation and provisioning operations.

Table 1-2 lists the default entries in this lookup definition.

Table 1-2 Entries in the Lookup.BMC.Configuration Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.bmc	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle class. Do *not* modify this entry.
Connector Name	org.identityconnectors.bmc.BMCConnector	This entry holds the name of the connector class. Do *not* modify this entry.

Table 1-2 (Cont.) Entries in the Lookup.BMC.Configuration Lookup Definition

Code Key	Decode	Description
defaultBatchSize	1000	This entry holds the number of records that must be included in each batch during batched reconciliation. This entry is used only when the Batch Size attribute of the user reconciliation scheduled jobs is either empty or set to 0. See Performing Batched Reconciliation for more information about the Batch Size attribute.
User Configuration Lookup	Lookup.BMC.UM.Configuration	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.

1.6.2.2 Lookup.BMC.Configuration.Trusted

The Lookup.BMC.Configuration.Trusted lookup definition holds connector configuration entries that are used during trusted source reconciliation.

Table 1-3 lists the default entries in this lookup definition.

Table 1-3 Entries in the Lookup.BMC.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Bundle Name	org.identityconnectors.bmc	This entry holds the name of the connector bundle package. Do *not* modify this entry.
Bundle Version	1.0.1115	This entry holds the version of the connector bundle class. Do *not* modify this entry.
Connector Name	org.identityconnectors.bmc.BMCConnector	This entry holds the name of the connector class. Do *not* modify this entry.
defaultBatchSize	1000	This entry holds the number of records that must be included in each batch during batched reconciliation. This entry is used only when the there is no value specified for the Batch Size attribute of the user reconciliation scheduled jobs. See Performing Batched Reconciliation for more information about the Batch Size attribute.
User Configuration Lookup	Lookup.BMC.UM.Configuration.Trusted	This entry holds the name of the lookup definition that contains user-specific configuration properties. Do *not* modify this entry.

1.6.2.3 Lookup.BMC.UM.Configuration

The Lookup.BMC.UM.Configuration lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a target resource.

Table 1-4 lists the default entries in this lookup definition.

Table 1-4 Entries in the Lookup.BMC.UM.Configuration Lookup Definition

Code Key	Decode	Description
Provisioning Attribute Map	Lookup.BMC.UM.ProvAttrMap	This entry holds the name of the lookup definition that maps process form fields and target system attributes. See Lookup.BMC.UM.ProvAttrMap for more information about this lookup definition.
Recon Attribute Map	Lookup.BMC.UM.ReconAttrMap	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.BMC.UM.ReconAttrMap for more information about this lookup definition.

1.6.2.4 Lookup.BMC.UM.Configuration.Trusted

The Lookup.BMC.UM.Configuration.Trusted lookup definition holds configuration entries that are specific to the user object type. This lookup definition is used during user management operations when your target system is configured as a trusted source.

Table 1-5 lists the default entries in this lookup definition.

Table 1-5 Entries in the Lookup.BMC.UM.Configuration.Trusted Lookup Definition

Code Key	Decode	Description
Recon Attribute Defaults	Lookup.BMC.UM.ReconDefaults.Trusted	This entry holds the name of the lookup definition that maps reconciliation fields and their default values. See Lookup.BMC.UM.ReconDefaults.Trusted for more information about this lookup definition.
Recon Attribute Map	Lookup.BMC.UM.ReconAttrMap.Trusted	This entry holds the name of the lookup definition that maps resource object fields and target system attributes. See Lookup.BMC.UM.ReconAttrMap.Trusted for more information about this lookup definition.

1.6.2.5 Lookup.BMC.UM.ProvAttrMap

The Lookup.BMC.UM.ProvAttrMap lookup definition holds mappings between process form fields and target system attributes. This lookup definitions is used during provisioning. This lookup definition is preconfigured. Table 1-17 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for provisioning. See Adding New Attributes for Provisioning.

1.6.2.6 Lookup.BMC.UM.ReconAttrMap

The Lookup.BMC.UM.ReconAttrMap lookup definition holds mappings between resource object fields and target system attributes. This lookup definition is used during reconciliation. This lookup definition is preconfigured. Table 1-14 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Adding New Attributes for Target Resource Reconciliation.

1.6.2.7 Lookup.BMC.UM.ReconAttrMap.Trusted

The Lookup.BMC.UM.ReconAttrMap.Trusted lookup definition holds mappings between resource object fields and target system attributes. This lookup definitions is used during trusted source user reconciliation runs. This lookup definition is preconfigured. Table 1-18 lists the default entries.

You can add entries in this lookup definitions if you want to map new target system attributes for reconciliation. See Adding New Attributes for Target Resource Reconciliation.

1.6.2.8 Lookup.BMC.UM.ReconDefaults.Trusted

The Lookup.BMC.UM.ReconDefaults.Trusted lookup definition holds mappings between reconciliation fields and their default values. This lookup definition is used when there is a mandatory field on the OIM User form, but no corresponding field in the target system from which values can be fetched during trusted source reconciliation.

Table 1-6 lists the default entries in this lookup definition.

Table 1-6 Entries in the Lookup.BMC.UM.ReconDefaults.Trusted Lookup Definition

Code Key	Decode
Employee Type	Full-Time
Organization	Xellerate Users
User Type	End-User

You add entries to this lookup definition in the following format, if required:

- **Code Key:** Name of the reconciliation field of the BMC user resource object
- **Decode:** Corresponding default value to be displayed

For example, assume a field named Preferred Language is a mandatory field on the OIM User form. Suppose the target system contains no field that stores information about the preferred language of a user account. During reconciliation, no value for the Preferred Language field is fetched from the target system. However, as the Preferred Language field cannot be left empty, you must specify a value for this field. Therefore, create an entry in this lookup definition with the Code Key value set to Preferred Language and Decode value set to English. This implies that the value of the Preferred Language field on the OIM User form displays English for all user accounts reconciled from the target system.

1.6.2.9 Lookup.BMC.ARLicenseType

The Lookup.BMC.ARLicenseType lookup definition maps possible values for the License Type attribute of the target system with the corresponding values to be displayed in the License Type field of the OIM User form.

Table 1-7 lists the default entries in this lookup definition.

Table 1-7 Entries in the Lookup.BMC.ARLicenseType Lookup Definition

Code Key	Decode
0	Read
1	Fixed
2	Floating

1.6.2.10 Lookup.BMC.ClientType

The Lookup.BMC.ClientType lookup definition maps possible values for the Client Type attribute of the target system with the corresponding values to be displayed in the Client Type field of the OIM User form.

Table 1-8 lists the default entries in this lookup definition.

Table 1-8 Entries in the Lookup.BMC.ClientType Lookup Definition

Code Key	Decode
10000	Vendor
2000	Office-Based Employee
3000	Field-Based Employee
4000	Home-Based Employee
5000	Contractor
7000	Customer
8000	Prospect

1.6.2.11 Lookup.BMC.SupportStaff

The Lookup.BMC.SupportStaff lookup definition maps possible values for the Support Staff attribute of the target system with the corresponding values to be displayed in the Support Staff field of the OIM User form.

Table 1-9 lists the default entries in this lookup definition.

Table 1-9 Entries in the Lookup.BMC.SupportStaff Lookup Definition

Code Key	Decode
0	Yes
1	No

1.6.2.12 Lookup.BMC.VIP

The Lookup.BMC.VIP lookup definition maps possible values for the VIP attribute of the target system with the corresponding values to be displayed in the VIP field of the OIM User form.

Table 1-10 lists the default entries in this lookup definition.

Table 1-10 Entries in the Lookup.BMC.VIP Lookup Definition

Code Key	Decode
0	Yes
1	No

1.6.2.13 Lookup.BMC.ClientSensitivity

The Lookup.BMC.ClientSensitivity lookup definition maps possible values for the Client Sensitivity attribute of the target system with the corresponding values to be displayed in the Client Sensitivity field of the OIM User form.

Table 1-11 lists the default entries in this lookup definition.

Table 1-11 Entries in the Lookup.BMC.ClientSensitivity Lookup Definition

Code Key	Decode
0	Sensitive
1	Standard

1.6.2.14 Lookup.BMC.ProfileStatus

The Lookup.BMC.ProfileStatus lookup definition maps possible values for the Profile Status attribute of the target system with the corresponding values to be displayed in the Profile Status field of the OIM User form.

Table 1-12 lists the default entries in this lookup definition.

Table 1-12 Entries in the Lookup.BMC.ProfileStatus Lookup Definition

Code Key	Decode
0	Proposed
1	Enabled
2	Offline
3	Obsolete
4	Archive
5	Delete

1.6.2.15 Lookup.BMC.HourlyRate

The Lookup.BMC.HourlyRate lookup definition maps possible values for the Hourly Rate attribute of the target system with the corresponding values to be displayed in the Hourly Rate Currency field of the OIM User form.

The following is the format of the Code Key and Decode values in this lookup definition:

- **Code:** Currency code
- **Decode:** Corresponding value to be displayed on the OIM User form

Table 1-13 lists the default entries in this lookup definition.

> **Note:**
>
> The entries listed in this lookup definition are entries for predefined currency codes available in the target system during installation. If the currency code list in the target system has been modified, then you must make the same changes to the entries in this lookup definition.

Table 1-13 Entries in the Lookup.BMC.HourlyRate Lookup Definition

Code Key	Decode
EUR	EUR - Euro
GBP	GBP -UK Pound Sterling
JPY	JPY - Japanese Yen
USD	USD -United States Dollar

1.7 Connector Objects Used During Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified accounts on the target system and using this data to add or modify resources assigned to OIM Users.

The BMC User Target Reconciliation scheduled job is used to initiate a target resource reconciliation run. This scheduled job is discussed in Scheduled Jobs for Reconciliation of User Records.

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about reconciliation

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

- User Fields for Target Resource Reconciliation
- Reconciliation Rule for Target Resource Reconciliation
- Reconciliation Action Rules for Target Resource Reconciliation

1.7.1 User Fields for Target Resource Reconciliation

The Lookup.BMC.UM.ReconAttrMap lookup definition maps resource object fields and target system attributes. This lookup definition is used for performing target resource user reconciliation runs.

In this lookup definition, entries are in the following format:

- **Code Key:** Reconciliation field of the resource object
- **Decode:** Name or ID of the target system attribute.

Table 1-14 provides information about user attribute mappings for target resource reconciliation.

Table 1-14 User Attributes for Target Resource Reconciliation

Resource Object Field	Target System Field
ARLicenseType	109
AssignmentAvailability	1000000346
ClientSensitivity	1000000027
ClientType	1000000022
Company[LOOKUP]	1000000001
Department[LOOKUP]	200000006
EmailAddress	1000000048
FirstName	1000000019
HourlyRateCurrency	hourlyRateCurrency
HourlyRateValue	hourlyRateValue
LastName	1000000018
LoginName	__NAME__
Organization[LOOKUP]	1000000010
PersonID	__UID__
PhoneNumber	1000000056
PrimaryCenterCode[LOOKUP]	300469300
ProfileStatus	7
Region[LOOKUP]	200000012
Site[LOOKUP]	260000001
SiteGroup[LOOKUP]	200000007
SiteID[LOOKUP]	1000000074
SupportGroup~SupportGroupID[LOOKUP]	supportGroup
SupportStaff	1000000025
Vip	1000000026

1.7.2 Reconciliation Rule for Target Resource Reconciliation

Learn about the reconciliation rule for this connector and how to view it.

- Target Resource Reconciliation Rule
- Viewing Target Resource Reconciliation Rules

1.7.2.1 Target Resource Reconciliation Rule

The following is the process-matching rule for this connector:

Rule name: BMC User Recon Rule

Rule element: User Login Equals LoginName

In this rule:

- User Login is the User ID attribute on the OIM User form.
- LoginName is the Login ID field of BMC.

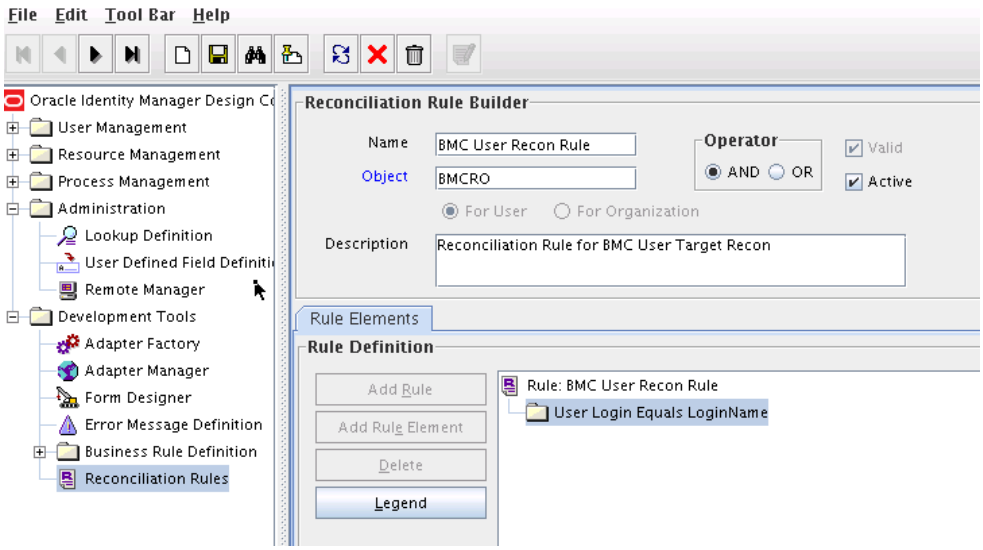
> **See Also:**
>
> Reconciliation Metadata in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for generic information about reconciliation matching and action rules

1.7.2.2 Viewing Target Resource Reconciliation Rules

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

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 Rule**. Figure 1-2 shows the reconciliation rule for target resource reconciliation.

Figure 1-2 Reconciliation Rule for Target Resource Reconciliation



1.7.3 Reconciliation Action Rules for Target Resource Reconciliation

Learn about the reconciliation action rules for this connector and how to view them.

- Target Resource Reconciliation Action Rules
- Viewing Target Resource Reconciliation Action Rules

1.7.3.1 Target Resource Reconciliation Action Rules

Table 1-15 lists the action rules for target resource reconciliation.

Table 1-15 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

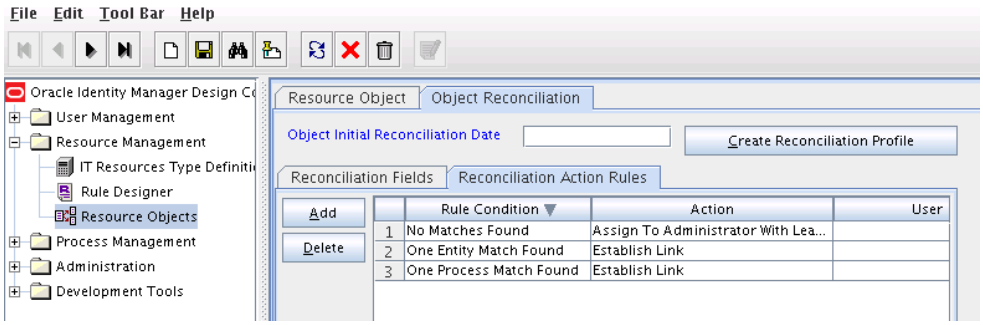
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see Defining Reconciliation Rules in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

1.7.3.2 Viewing Target Resource Reconciliation Action Rules

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

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



1.8 Connector Objects Used During Provisioning

Provisioning involves creating or modifying user data on the target system through Oracle Identity Manager.

This section discusses the following topics:

- Provisioning Functions
- User Fields for Provisioning

1.8.1 Provisioning Functions

Table 1-16 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 1-16 Provisioning Functions

Function	Adapter
Create User	CreateBMCUser
Delete User	DeleteBMCUser

Table 1-16 (Cont.) Provisioning Functions

Function	Adapter
Update User	UpdateBMCUser
Reset User Password	UpdateBMCUser
Add Support Group	BMCAddGroup
Delete Support Group	RemoveBMCSupportGroup
Update Support Group	BMCUpdateSupportGroup

1.8.2 User Fields for Provisioning

The Lookup.BMC.UM.ProvAttrMap lookup definition maps process form fields with target system attributes. This lookup definition is used for performing user provisioning operations.

> **Note:**
>
> The HourlyRateCurrency and HourlyRateValue fields on the OIM User process form have default values which are same as the values in the target system. During a Create User provisioning operation, you can modify the values for these fields. If the value in these fields are cleared and no new values are provided, then the default values will be honored while creating a new user on the target system. Note that you can clear the value in these fields only during an update provisioning operation.

Table 1-17 lists the user identity fields of the target system for which you can specify or modify values during provisioning operations.

Table 1-17 Entries in the Lookup.BMC.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
ARLicenseType	109
BusinessPhone	1000000056
ClientSensitivity	1000000027
ClientType	1000000022
Company[LOOKUP]	1000000001
Department[LOOKUP]	200000006
Email	1000000048
FirstName	1000000019
HourlyRateCurrency[IGNORE]	IGNORE
HourlyRateValue	240000040=(HourlyRateValue !=null && HourlyRateCurrency != null) ? (HourlyRateValue+" "+HourlyRateCurrency):null

Table 1-17 (Cont.) Entries in the Lookup.BMC.UM.ProvAttrMap Lookup Definition

Process Form Field	Target System Field
LastName	1000000018
LoginName	__NAME__
Organization[LOOKUP]	1000000010
Password	__PASSWORD__
PersonID	__UID__
PrimaryCenterCode[LOOKUP]	300469300
ProfileStatus	7
Region[LOOKUP]	200000012
Site[LOOKUP]	260000001
SiteGroup[LOOKUP]	200000007
SiteID[LOOKUP]	1000000074
SupportStaff	1000000025
UD_BMC_GRP~SupportGroupID[LOOKUP]	1000000079
VIP	1000000026

1.9 Connector Objects Used During Trusted Source Reconciliation

Trusted source reconciliation involves fetching data about newly created or modified accounts on the target system and using that data to create or update OIM Users.

> **See Also:**
>
> Trusted Source Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for conceptual information about trusted source reconciliation

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

- User Fields for Trusted Source Reconciliation
- Reconciliation Rule for Trusted Source Reconciliation
- Reconciliation Action Rules for Trusted Source Reconciliation

1.9.1 User Fields for Trusted Source Reconciliation

The Lookup.BMC.UM.ReconAttrMap.Trusted lookup definition maps user fields of the OIM User form with corresponding field names in the target system. This lookup definition is used for performing trusted source reconciliation runs.

Table 1-18 lists user attributes for trusted source reconciliation.

Table 1-18 Entries in the Lookup.BMC.UM.ReconAttrMap.Trusted Lookup Definition

OIM User Form Field	Target System Field
Last Name	1000000018
User ID	__NAME__

1.9.2 Reconciliation Rule for Trusted Source Reconciliation

Learn about the reconciliation rule for trusted source reconciliation and how to view it.

- Trusted Source Reconciliation Rule
- Viewing Trusted Source Reconciliation Rule

1.9.2.1 Trusted Source Reconciliation Rule

> **See Also:**
>
> Managing Reconciliation in *Oracle Fusion Middleware Administering Oracle Identity Manager* for generic information about reconciliation matching and action rules

The following is the process matching rule:

Rule name: BMC User Trusted Recon Rule

Rule element: User Login Equals User ID

In this rule element:

- User Login is the User ID field on the OIM User form.
- User ID is the Login ID field of BMC.

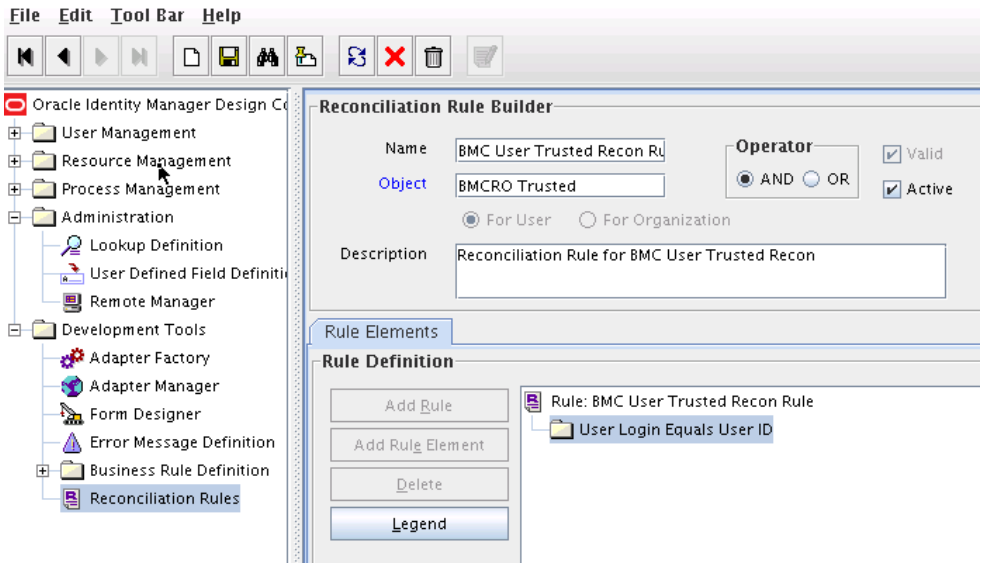
1.9.2.2 Viewing Trusted Source Reconciliation Rule

You can view the reconciliation rule for trusted source reconciliation by performing the following steps after you deploy the connector:

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.

3. Double-click **Reconciliation Rules**.
4. Search for **BMC User Trusted Recon Rule**. Figure 1-4 shows the reconciliation rule for trusted source reconciliation.

Figure 1-4 Reconciliation Rule for Trusted Source Reconciliation



1.9.3 Reconciliation Action Rules for Trusted Source Reconciliation

Learn about the reconciliation action rules for trusted source reconciliation and how to view them.

- Trusted Source Reconciliation Action Rules
- Viewing Trusted Source Reconciliation Action Rules

1.9.3.1 Trusted Source Reconciliation Action Rules

Table 1-19 lists the action rules for target resource reconciliation.

Table 1-19 Action Rules for Trusted Source Reconciliation

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

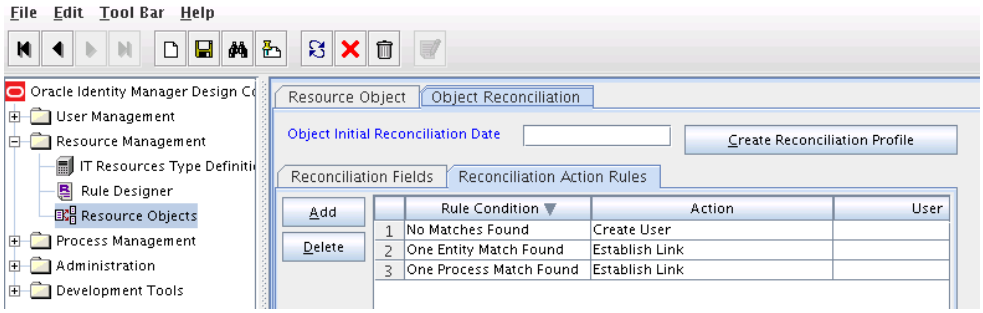
> **Note:**
>
> No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. See Defining Reconciliation Rules in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about modifying or creating reconciliation action rules.

1.9.3.2 Viewing Trusted Source Reconciliation Action Rules

You can view the reconciliation action rules for trusted source reconciliation by performing the following steps after you deploy the connector:

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 Trusted** 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



2
Deploying the Connector

The procedure to deploy the connector can be divided into these stages.

- Preinstallation
- Installation
- Postinstallation
- Upgrading the Connector

2.1 Preinstallation

Preinstallation involves performing procedures such as copying external code files on Oracle Identity Manager, configuring encryption security on the target system, and so on.

- Copying the External Code Files
- Creating a Target System User Account for Connector Operations
- Understanding and Configuring Encryption Security

2.1.1 Copying the External Code Files

You must copy the external code files as follows:

1. Create a directory named BMC-***RELEASE_NUMBER*** under the following directory:

   OIM_HOME/server/ConnectorDefaultDirectory/targetsystems-lib/

   For example, if you are using release 11.1.1.5.0 of this connector, then create a directory named BMC-11.1.1.5.0 in the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib/.

2. Copy the arapi***VERSION_NUM***.jar (replace *VERSION_NUM* with the release number of the target system that you are using) and log4j-1.2.14.jar files from the BMC Remedy Admin Client installation directory to the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib/BMC-***RELEASE_NUMBER.***

   For example, if you are using BMC Remedy AR System 8.0.00 as the target system, then copy the arapi80_build001.jar file from the *BMC_INSTALL_DIR*\BMC Software\ARSystem\Arserver\api\lib directory to the *OIM_HOME*/server/ConnectorDefaultDirectory/targetsystems-lib/BMC-***RELEASE_NUMBER*** directory.

   Similarly, if you are using BMC Remedy AR System 7.6.04 as the target system, then copy the arapi7604_build002.jar file.

2.1.2 Creating a Target System User Account for Connector Operations

Oracle Identity Manager requires a target system user account to access the target system during reconciliation and provisioning operations. You provide the credentials of this user account while performing the procedure described in Configuring the IT Resource for the Target System.

The target system user account for connector operations must have the following permissions:

- Contact Organization Admin
- Administrator
- Check Unrestricted Access under Login/Access Details
- User must have fixed (write) license

To assign these minimum permissions:

1. Log in to BMC Remedy Action Request System.
2. In the left navigation pane, click **Administration Console,** and then click **Application Administration Console.**
3. On the Standard Configuration tab, from the Configuration for Company list, select the name of the company to which the user account to be used for connector operations belongs.
4. Click the View link corresponding to the People entry.
5. From the list of users that is displayed in the upper horizontal pane, select the user account to be used for connector operations.

   The user details are displayed on the Person ID form in the lower pane.
6. On the Login/Access Details tab, click **Update Permissions Group.**
7. In the Permission Groups Update window, from the Permission Group list, select **AR System,** and then **Administrator.**
8. Click **Add/Modify.** The Administrator permission group is added to and displayed in the Permission Group region.
9. From the Permission Group list, select **Foundation,** and then **Contact Organization Admin.**
10. Click **Add/Modify.** The Contact Organization Admin permission group is added to and displayed in the Permission Group region.
11. Click **Close.**

2.1.3 Understanding and Configuring Encryption Security

Learn about the various encryption options for your target system and how to configure encryption.

> **Note:**
>
> If you are using BMC Remedy AR System 7.1 as the target system, then to configure encryption you must modify the ar.conf (UNIX) or ar.cfg (Microsoft Windows) configuration file. See the target system documentation for complete information about configuring encryption.

- Understanding the Encryption Security Options on the Encryption Tab
- Understanding the Encryption Options in the New Encryption Settings Section
- Configuring Encryption

2.1.3.1 Understanding the Encryption Security Options on the Encryption Tab

You use the Encryption tab to understand and configure encryption security options such as the following:

> **See Also:**
>
> The target system documentation for detailed information about topics discussed in this section

- **Encryption Level Available**

  > **Note:**
  >
  > If the level of encryption is Standard, then you must just enable encryption on the BMC Remedy Server (server). There is no need not perform any more procedures on the client side. For all other levels of encryption, see the target system guide for information of procedures to be performed on client side.

  This field displays the level of encryption currently installed on the BMC Remedy Server (server). The following are the levels of encryption available:

  – **Standard:** This is the default and standard level of encryption.

  – **Performance:** This is the BMC Remedy Encryption Performance Security.

  – **Premium:** This is the BMC Remedy Encryption Premium Security.

  The default encryption level is `Standard`.

- **Active Encryption Settings**

  This section contains a set of read-only fields that display the current encryption settings on the target system.

- **New Encryption Settings**

This section contains a set of fields that you use to modify the encryption settings on your target system. All values that you specify in this section are saved to the target system configuration files ar.conf (UNIX) or ar.cfg (Microsoft Windows). In addition, these values are displayed in the Active Encryption Settings section.

2.1.3.2 Understanding the Encryption Options in the New Encryption Settings Section

The following sections provide more information on the encryption options that you can set in the New Encryption Settings section:

- Security Policy
- Data Key Details
- Public Key Details

2.1.3.2.1 Security Policy

The following are the values that you can select from the Security Policy list:

- **Optional**

  When you select this option, clients can communicate with the server irrespective of whether or not encryption is installed. If the client supports server encryption configuration, then network traffic is encrypted. Otherwise, plain text is used in the network traffic.

  This is the default selection for BMC Remedy Encryption Performance Security and BMC Remedy Encryption Premium Security FIPS noncompliance.

  The following is the setting in the server configuration file:

  ```
  Encrypt-Security-Policy: 0
  ```

- **Required**

  When you select this option, clients can communicate with the server only if encryption is installed.

  This is the default selection for BMC Remedy Encryption Performance Security and BMC Remedy Encryption Premium Security FIPS compliance.

  Note that the encryption algorithms used by the server must be compatible with the encryption level installed on the client.

  The following is the setting in the server configuration file:

  ```
  Encrypt-Security-Policy: 1
  ```

- **Disabled**

  When you select this option, communication with the server is not encrypted irrespective of whether or not encryption is installed on the client. Plain text is exchanged in network traffic.

  The following is the setting in the server configuration file

  ```
  Encrypt-Security-Policy: 2
  ```

2.1.3.2.2 Data Key Details

After the connection between the sever and clients is established, the data exchanged is processed by the data key. In this region, you specify values for the following UI elements to configure the cryptographic algorithm and size of the data key:

- **Algorithm Options**

  Select one of the following options to specify the data encryption algorithm:

  > **Note:**
  >
  > Depending on the level of encryption installed on the server and whether FIPS is enabled, you can see one or more algorithms discussed in this section.

  - **DES:** This is the 56-bit Data Encryption Standard (DES) algorithm using Cipher Block Chaining (CBC) mode.

    The following is the setting in the server configuration file:

    ```
    Encrypt-Data-Encryption-Algorithm: 1
    ```

  - **RC4-128:** This is the 128-bit RC4 key algorithm. This algorithm is available for BMC Remedy Encryption Performance Security that does not comply with FIPS.

    The following is the setting in the server configuration file:

    ```
    Encrypt-Data-Encryption-Algorithm: 2
    ```

  - **RC4-2048:** This is the 2048-bit RC4 key algorithm. This algorithm is available for BMC Remedy Encryption Premium Security that does not comply with FIPS.

    The following is the setting in the server configuration file:

    ```
    Encrypt-Data-Encryption-Algorithm: 3
    ```

  - **AES-128:** This is the 128-bit AES CBC key algorithm. This algorithm is mandatory for BMC Remedy Encryption Performance Security that complies with FIPS. However, servers that do not comply with FIPS can also use this algorithm.

    The following is the setting in the configuration file of a server that does not comply with FIPS:

    ```
    Encrypt-Data-Encryption-Algorithm: 6
    ```

    The following is the setting in the configuration file of a server that complies with FIPS:

    ```
    Encrypt-Data-Encryption-Algorithm: 8
    ```

  - **AES-256:** This is the 256-bit AES CBC key algorithm. This algorithm is mandatory for BMC Remedy Encryption Premium Security that complies with FIPS. However, servers that do not comply with FIPS can also use this algorithm.

The following is the setting in the configuration file of a server that does not comply with FIPS:

```
Encrypt-Data-Encryption-Algorithm: 7
```

The following is the setting in the configuration file of a server that complies with FIPS:

```
Encrypt-Data-Encryption-Algorithm: 9
```

- **Key Expire Interval**

  Enter an integer value in this field. This value represent the life span of the key in seconds. The key expires after the specified time (in seconds) is reached, and then exchange of a new key happens.

  Note that this is an optional field and its default value is `2700` seconds. The following is the setting in the server configuration file:

  ```
  Encrypt-Symmetric-Data-Key-Expire: 2700
  ```

2.1.3.2.3 Public Key Details

When the data encryption key expires and the API session is about to begin, an private keys establishment (exchange of private keys) occurs. In order to establish or exchange private keys, BMC Remedy Encryption Performance Security and BMC Remedy Encryption Premium Security use the RSA algorithm for public key cryptography. In this region, you specify values for the following UI elements to configure the cryptographic algorithm and size of the public key:

- **Algorithm Options**

  Select one of the following options to specify the data encryption algorithm:

  > **Note:**
  >
  > Depending on the level of encryption installed on the server and whether FIPS is enabled, you can see one or more algorithms discussed in this section.

  – **RSA 512:** This is the 512-bit RSA key algorithm and is the default value for standard security.

    The following is the setting in the server configuration file:

    ```
    Encrypt-Public-Key-Algorithm: 4
    ```

  – **RSA 1024:** This is the 1024-bit RSA key algorithm and is the default value for BMC Remedy Encryption Performance Security.

    The following is the setting in the server configuration file:

    ```
    Encrypt-Public-Key-Algorithm: 5
    ```

  – **RSA 2048:** This is the 2048-bit RSA key algorithm and is the default value for BMC Remedy Encryption Premium Security.

    The following is the setting in the server configuration file:

    ```
    Encrypt-Public-Key-Algorithm: 6
    ```

- **Key Expire Interval**

  Enter an integer value in this field. This value represent the life span of the key in seconds. The key expires after the specified time (in seconds) is reached, and then the server generates a new key.

  Note that this is an optional field and its default value is `86400` seconds. The following is the setting in the server configuration file:

  ```
  Encrypt-Symmetric-Data-Key-Expire: 86400
  ```

2.1.3.3 Configuring Encryption

Before you proceed with installing the connector, you can configure encryption on the target system. You can review and configure the encryption options for your target system as follows:

1. Log in to BMC Remedy Action Request System.
2. In the left navigation pane, click **AR System Administration,** and then click **AR System Administration Console.**
3. In the left pane of the new window that is displayed, click **System, General,** and then click **Server Information.**
4. In the Server Information form, click the **Encryption** tab. You can review and configure your encryptions options in this tab.

> **See Also:**
>
> Understanding the Encryption Security Options on the Encryption Tab for the list of available options to configure encryption

2.2 Installation

Depending on where you want to run the connector code (bundle), the connector provides these installation options.

- To run the connector code locally in Oracle Identity Manager, perform the procedure described in Installing the Connector in Oracle Identity Manager.
- To run the connector code remotely in a Connector Server, perform the procedures described in Installing the Connector in Oracle Identity Manager and Deploying the Connector in a Connector Server.

2.2.1 Installing the Connector in Oracle Identity Manager

Installation on Oracle Identity Manager consists of the following procedures:

- Running the Connector Installer
- Configuring the IT Resource for the Target System

2.2.1.1 Running the Connector Installer

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

To run the Connector Installer:

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

   OIM_HOME/server/ConnectorDefaultDirectory

2. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   a. Log in to the Administrative and User Console.
   b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector.**
3. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. Log in to Oracle Identity System Administration.
   b. In the left pane, under System Management, click **Manage Connector.**
4. In the Manage Connector page, click **Install.**
5. From the Connector List list, select **BMC Remedy User Management Connector *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 Connector *RELEASE_NUMBER.***
6. Click **Load**.
7. 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 is 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.

8. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of 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 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

      The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled jobs

      The procedure to configure these scheduled jobs 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 A-1.

2.2.1.2 Configuring the IT Resource for the Target System

> **Note:**
>
> If you have configured your target system as a trusted source, then create an IT resource of type **BMCRemedy.** For example, BMCRemedy Trusted. The parameters of this IT resource are the same as the parameters of the IT resources described in Table 2-1 of this section. See *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about creating an IT resource.

The IT resource for the target system is created during connector installation. This IT resource contains connection information about the target system. Oracle Identity Manager uses this information during reconciliation and provisioning.

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

1. If you are using Oracle Identity Manager release 11.1.1.*x,* then:

   a. Log in to the Administrative and User Console

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

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

2. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:

   a. Log in to Oracle Identity System Administration

   b. In the left pane, under Configuration, click **IT Resource.**

3. In the IT Resource Name field on the Manage IT Resource page, enter `BMCRemedy Server` and then click **Search**. Figure 2-1 shows the Manage IT Resource page.

Figure 2-1 Manage IT Resource Page

4. Click the edit icon corresponding to the BMCRemedy Server IT resource.

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

6. Specify values for the parameters of the BMCRemedy Server IT resource. Figure 2-2 shows the Edit IT Resource Details and Parameters page.

Figure 2-2 Edit IT Resource Details and Parameters Page for the BMCRemedy Server IT Resource

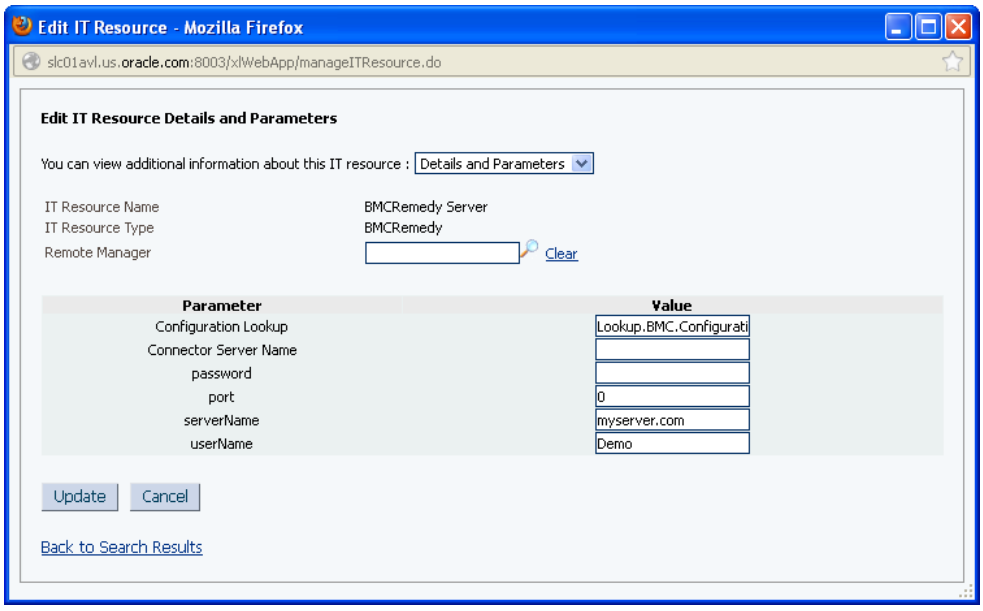


Table 2-1 describes each parameter of the BMCRemedy Server IT resource.

Table 2-1 Parameters of the BMCRemedy Server IT Resource for the Target System

Parameter	Description
Configuration Lookup	This parameter holds the name of the lookup definition that stores configuration information used during reconciliation and provisioning. If you have configured your target system as a target resource, then enter `Lookup.BMC.Configuration`. If you have configured your target system as a trusted source, then enter `Lookup.BMC.Configuration.Trusted`. Default value: `Lookup.BMC.Configuration`
Connector Server Name	Name of the IT resource of the type "Connector Server." You create an IT resource for the Connector Server in Creating the IT Resource for the Connector Server. **Note:** Enter a value for this parameter only if you have deployed the BMC User Management connector in the Connector Server. Sample value: `BMC Connector Server`
Password	Enter the password of the user account that you create by performing the procedure described in Creating a Target System User Account for Connector Operations.
Port	Enter the TCP/IP port at which the BMC Remedy server is listening. Default value: `0` **Note:** You must specify a value for this parameter *only* if the BMC Remedy server is not registered with the port mapper. You need not specify a value for this parameter if the BMC Remedy server is registered with the port mapper.
serverName	Enter the IP address or computer name of the BMC Remedy User Management server.

Table 2-1 (Cont.) Parameters of the BMCRemedy Server IT Resource for the Target System

Parameter	Description
userName	Enter the User ID of the user account that you created by performing the procedure described in Creating a Target System User Account for Connector Operations. Default value: `Demo`

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

2.2.2 Deploying the Connector in a Connector Server

You can deploy the BMC User Management connector either locally in Oracle Identity Manager or remotely in the Connector Server. A **connector server** is an application that enables remote execution of an Identity Connector, such as the BMC User Management connector.

> **Note:**
>
> - To deploy the connector bundle remotely in a Connector Server, you must first deploy the connector in Oracle Identity Manager, as described in Installing the Connector in Oracle Identity Manager.
> - See Creating the IT Resource for the Connector Server for related information.

This procedure can be divided into the following stages:

- Installing and Configuring the Connector Server
- Running the Connector Server
- Installing the Connector on the Connector Server

2.2.2.1 Installing and Configuring the Connector Server

Connector servers are available in two implementations:

- As a .Net implementation that is used by Identity Connectors implemented in .Net
- As a Java Connector Server implementation that is used by Java-based Identity Connectors

The BMC User Management connector is implemented in Java, so you can deploy this connector to a Java Connector Server.

Use the following steps to install and configure the Java Connector Server:

> **Note:**
>
> Before you deploy the Java Connector Server, ensure that you install the JDK or JRE on the same computer where you are installing the Java Connector Server and that your *JAVA_HOME* or *JRE_HOME* environment variable points to this installation.

1. Create a new directory on the computer where you want to install the Java Connector Server.

   > **Note:**
   >
   > In this guide, *CONNECTOR_SERVER_HOME* represents this directory.

2. Unzip the Java Connector Server package in the new directory created in Step 1. You can download the Java Connector Server package from the Oracle Technology Network.
3. Open the ConnectorServer.properties file located in the `conf` directory. In the ConnectorServer.properties file, set the following properties, as required by your deployment.

Property	Description
connectorserver.port	Port on which the Java Connector Server listens for requests. Default is `8763`.
connectorserver.bundleDir	Directory where the connector bundles are deployed. Default is `bundles`.
connectorserver.libDir	Directory in which to place dependent libraries. Default is `lib`.
connectorserver.usessl	If set to **`true`**, the Java Connector Server uses SSL for secure communication. Default is `false`. If you specify **`true`**, use the following options on the command line when you start the Java Connector Server: • `-Djavax.net.ssl.keyStore` • `-Djavax.net.ssl.keyStoreType` (*optional*) • `-Djavax.net.ssl.keyStorePassword`
connectorserver.ifaddress	Bind address. To set this property, uncomment it in the file (if necessary). The bind address can be useful if there are more NICs installed on the computer.
connectorserver.key	Java Connector Server key.

4. Set the properties in the ConnectorServer.properties file, as follows:
   - To set the connectorserver.key, run the Java Connector Server with the `/setKey` option.

> **Note:**
>
> See Running the Connector Server.

- For all other properties, edit the ConnectorServer.properties file manually.

5. The conf directory also contains the logging.properties file, which you can edit if required by your deployment.

> **Note:**
>
> Oracle Identity Manager has no built-in support for connector servers, so you cannot test your configuration.

2.2.2.2 Running the Connector Server

To run the Java Connector Server, use the ConnectorServer.bat script for Windows and use the ConnectorServer.sh script for UNIX as follows:

1. Make sure that you have set the properties required by your deployment in the ConnectorServer.properties file, as described in Installing and Configuring the Connector Server.
2. Change to the *CONNECTOR_SERVER_HOME*\bin directory and find the ConnectorServer.bat script.

   The ConnectorServer.bat supports the following options:

Option	Description
`/install [serviceName] ["-J java-option"]`	Installs the Java Connector Server as a Windows service. Optionally, you can specify a service name and Java options. If you do not specify a service name, the default name is `ConnectorServerJava`.
`/run ["-J java-option"]`	Runs the Java Connector Server from the console. Optionally, you can specify Java options. For example, to run the Java Connector Server with SSL: `ConnectorServer.bat /run "-J-Djavax.net.ssl.keyStore=mykeystore.jks" "-J-Djavax.net.ssl.keyStorePassword=password"`
`/setKey [key]`	Sets the Java Connector Server key. The `ConnectorServer.bat` script stores the hashed value of the key in the `connectorserver.key` property in the `ConnectorServer.properties` file.
`/uninstall [serviceName]`	Uninstalls the Java Connector Server. If you do not specify a service name, the script uninstalls the `ConnectorServerJava` service.

3. If you need to stop the Java Connector Server, stop the respective Windows service.

2.2.2.3 Installing the Connector on the Connector Server

> **See Also:**
>
> Using an Identity Connector Server in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about installing and configuring connector server and running the connector server

If you need to deploy the BMC User Management connector into the Java Connector Server, then follow these steps:

1. Stop the Java Connector Server.

   > **Note:**
   >
   > - You can download the necessary Java Connector Server from the Oracle Technology Network web page.
   > - Ensure that you are using latest framework JARs of Oracle Identity Manager to keep the Connector Server consistent with your Oracle Identity Manager instance. To do so:
   >
   >   Copy the framework JAR files, connector-framework.jar and connector-framework-internal.jar, from the *OIM_HOME*/server/ext/internal directory to the *CONNECTOR_SERVER_HOME*/lib/framework directory.

2. Copy the connector bundle JAR file (org.identityconnectors.bmc-1.0.1115.jar) from the installation media into the Java Connector Server *CONNECTOR_SERVER_HOME*/bundles directory.
3. Copy the following files from the BMC Remedy Admin Client installation directory into the *CONNECTOR_SERVER_HOME*/lib directory:
   - arapi***VERSION_NUM***.jar
   - log4j-1.2.14.jar
4. Start the Java Connector Server.

2.3 Postinstallation

Postinstallation involves performing certain procedures such as configuring Oracle Identity Manager, creating the IT resource for the Connector Server, enabling logging, localizing field labels, and so on.

- Configuring Oracle Identity Manager 11.1.2 or Later
- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Managing Logging

- Setting up the Lookup Definition for Connection Pooling
- Configuring Oracle Identity Manager for Request-Based Provisioning
- Localizing Field Labels in UI Forms
- Creating the IT Resource for the Connector Server

2.3.1 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs.

These procedures are described in the following sections:

- Creating and Activating a Sandbox
- Creating a New UI Form
- Creating an Application Instance
- Publishing a Sandbox
- Harvesting Entitlements and Sync Catalog
- Configuring the Password Form Field

2.3.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows:

1. Log in to Oracle Identity System Administration.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.
3. On the toolbar, click **Create Sandbox.**
4. In the Create Sandbox dialog box, enter values for the following fields:
   - **Sandbox Name:** Enter a name for the sandbox.
   - **Sandbox Description:** Enter a description of the sandbox.
5. Click **Save and Close.**
6. Click **OK** on the confirmation message that is displayed.

   The sandbox is created and displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
8. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

2.3.1.2 Creating a New UI Form

Create a new UI form as follows:

1. In the left pane, under Configuration, click **Form Designer.** The Form Designer page is displayed.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Form page is displayed.
3. On the Create Form page, enter values for the following UI fields:
   - **Resource Type:** Select the resource object that you want to associate the form with. For example, **BMCRO.**
   - **Form Name:** Enter a name for the form.
4. Click **Create.**

   A message is displayed stating that the form is created.

2.3.1.3 Creating an Application Instance

Create an application instance as follows:

1. In the left pane of the System Administration console, under Configuration, click **Application Instances.** The Application Instances page is displayed.
2. From the Actions menu, select **Create.** Alternatively, click **Create** on the toolbar. The Create Application Instance page is displayed.
3. Specify values for the following fields:
   - **Name:** The name of the application instance.
   - **Display Name:** The display name of the application instance.
   - **Description:** A description of the application instance.
   - **Resource Object:** The resource object name. Click the search icon next to this field to search for and select **BMCRO.**
   - **IT Resource Instance:** The IT resource instance name. Click the search icon next to this field to search for and select **BMCRemedy Server.**
   - **Form:** Select the form name (created in Creating a New UI Form).
4. Click Save. The application instance is created.
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See Managing Organizations Associated With Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed instructions.

2.3.1.4 Publishing a Sandbox

To publish the sandbox that you created in Creating and Activating a Sandbox:

1. Close all the open tabs and pages.
2. In the upper right corner of the page, click the **Sandboxes** link.

   The Manage Sandboxes page is displayed.
3. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Creating and Activating a Sandbox.
4. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.

5. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.3.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization listed in Scheduled Job for Lookup Field Synchronization.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.3.1.6 Configuring the Password Form Field

After installing the connector, you must add and set the value of the AccountPassword property to true in the UD_BMC process form.

To do so:

1. Log in to the Design Console.
2. Expand **Development Tools,** and double-click **Form Designer.**
3. Search for and open the **UD_BMC** process form.
4. Click **Create New Version.**
5. In the Label field, enter the version name. For example, `version#1.`
6. Click the Save icon.
7. Select the current version created in Step 4 from the **Current Version** list.
8. On the Properties tab, search for and select the Password field (UD_BMC_PWD), and then click **Add Property.**

   The Add Property dialog box is displayed.
9. From the Property Name list, select **AccountPassword.**
10. In the Property Value field, enter `true.`
11. Click the Save icon and close the dialog box.
12. Click the Save icon to save the form.
13. Click **Make Version Active.**

2.3.2 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 Oracle Identity Manager database. 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, 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:
>
> *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
> ```

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.

2.3.3 Managing Logging

Oracle Identity Manager uses the Oracle Diagnostic Logging (ODL) logging service for recording all types of events pertaining to the connector.

The following topics provide detailed information about logging:

- Understanding Log Levels

- Enabling Logging

2.3.3.1 Understanding Log Levels

Oracle Identity Manager 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 2-2.

Table 2-2 Log Levels and ODL Message Type:Level Combinations

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

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

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

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

2.3.3.2 Enabling Logging

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="org.identityconnectors.bmc" 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 2-2 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="org.identityconnectors.bmc" 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.

2.3.4 Setting up the Lookup Definition for Connection Pooling

By default, this connector uses the ICF connection pooling. Table 2-3 lists the connection pooling properties, their description, and default values set in ICF:

Table 2-3 Connection Pooling Properties

Property	Description
Pool Max Idle	Maximum number of idle objects in a pool. Default value: `10`
Pool Max Size	Maximum number of connections that the pool can create. Default value: `10`
Pool Max Wait	Maximum time, in milliseconds, the pool must wait for a free object to make itself available to be consumed for an operation. Default value: `150000`
Pool Min Evict Idle Time	Minimum time, in milliseconds, the connector must wait before evicting an idle object. Default value: `120000`
Pool Min Idle	Minimum number of idle objects in a pool. Default value: `1`

If you want to modify the connection pooling properties to use values that suit requirements in your environment, then:

1. Log in to the Design Console.
2. Expand **Administration,** and then double-click **Lookup Definition.**
3. Search for and open one of the following lookup definitions:

   For the trusted source mode: **Lookup.BMC.Configuration.Trusted**

   For target resource mode: **Lookup.BMC.Configuration**
4. On the Lookup Code Information tab, click **Add.**

   A new row is added.
5. In the **Code Key** column of the new row, enter `Pool Max Idle.`
6. In the **Decode** column of the new row, enter a value corresponding to the Pool Max Idle property.
7. Repeat Steps 4 through 6 for adding each of the connection pooling properties listed in Table 2-3.

8. Click the Save icon.

2.3.5 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.*x*.

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 BMC Remedy 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:

- Importing Request Datasets
- Enabling the Auto Save Form Feature
- Running the PurgeCache Utility

2.3.5.1 Importing Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation.

There are two ways of importing request datasets:

- Importing Request Datasets into MDS
- Importing Request Datasets Using Deployment Manager

> **Note:**
>
> Request datasets imported either into MDS or by using Deployment Manager are same.

2.3.5.1.1 Importing Request Datasets into MDS

To import a request dataset definition into the metadata store (MDS):

1. Copy the predefined request dataset from the installation media to any directory on the Oracle Identity Manager host computer. The predefined request dataset is available in the xml/BMCRemedy-Datasets.xml file on the installation media. It is recommended that you create a directory structure as follows:

   /custom/connector/*RESOURCE_NAME*

   For example:

   E:\MyDatasets\custom\connector\BMC

   > **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 BMCRemedy-Datasets.xml file is the MDS location into which this file is imported after you run the Oracle Identity Manager MDS Import utility.

2. Ensure that you have set the environment for running the MDS Import utility. See Exporting All MDS Data for Oracle Identity Manager in *Oracle Fusion Middleware Developing and Customizing Applications 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 Step 1 of this procedure, if you copy the files to the E:\MyDatasets\custom\connector\BMC directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

3. In a command window, change to the *OIM_HOME*\server\bin directory.
4. Run one of the following commands:
   - On Microsoft Windows

```
weblogicImportMetadata.bat
```

- On UNIX

```
weblogicImportMetadata.sh
```

5. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to WebLogic server

     Sample value: `WL_User`
   - `Please enter your password [weblogic]`

     Enter the password used to log in to 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.

2.3.5.1.2 Importing Request Datasets Using Deployment Manager

The request datasets (predefined or generated) can also be imported by using the Deployment Manager (DM). The predefined request datasets are stored in the xml directory on the installation media.

To import a request dataset definition by using the Deployment Manager:

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 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 BMCRemedy-Datasets file, which is located in the xml directory of 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**.

The request datasets are imported into MDS.

2.3.5.2 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.

2.3.5.3 Running the PurgeCache Utility

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

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

2.3.6 Localizing Field Labels in UI Forms

You can localize UI form field labels by using the resource bundle corresponding to the language you want to use. The resource bundles are available in the connector installation media.

> **Note:**
>
> Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.*x* or later and you want to localize UI form field labels.

To localize field label that you add to in UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor:
   - For Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle_en.xlf
   - For releases prior to Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0):

     SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file in the following manner:

a. Search for the following text:

```
<file source-language="en"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

b. Replace with the following text:

```
<file source-language="en" target-language="LANG_CODE"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

In this text, replace *LANG_CODE* with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

```
<file source-language="en" target-language="ja"
original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
datatype="x-oracle-adf">
```

c. Search for the application instance code. This procedure shows a sample edit for BMCFORM application instance. The original code is:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_B
MC_LOGINNAME__c_description']}">
<source>LoginName</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.BMCFORM.entity.BMCFORMEO.UD_B
MC_LOGINNAME__c_LABEL">
<source>LoginName</source>
<target/>
</trans-unit>
```

d. Open the resource file from the connector package, for example BMCRemedy-UM_ja.properties, and get the value of the attribute from the file, for example, global.udf.UD_BMC_LOGINNAME=\u30ED \u30B0\u30A4\u30F3\u540D.

e. Replace the original code shown in Step 6.c with the following:

```
<trans-unit id="$
{adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBundle']
['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.userEO.UD_B
MC_LOGINNAME__c_description']}">
<source>LoginName</source>
<target>\u30ED\u30B0\u30A4\u30F3\u540D<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.BMCFORM.entity.BMCFORMEO.UD_B
MC_LOGINNAME__c_LABEL">
<source>LoginName</source>
<target>\u30ED\u30B0\u30A4\u30F3\u540D<target/>
</trans-unit>
```

f. Repeat Steps 6.c through 6.e for all attributes of the process form.

g. Save the file as BizEditorBundle_*LANG_CODE*.xlf. In this file name, replace *LANG_CODE* with the code of the language to which you are localizing.

Sample file name: BizEditorBundle_ja.xlf.

7. Repackage the ZIP file and import it into MDS.

> **See Also:**
>
> Deploying and Undeploying Customizations in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager,* for more information about exporting and importing metadata files

8. Log out of and log in to Oracle Identity Manager.

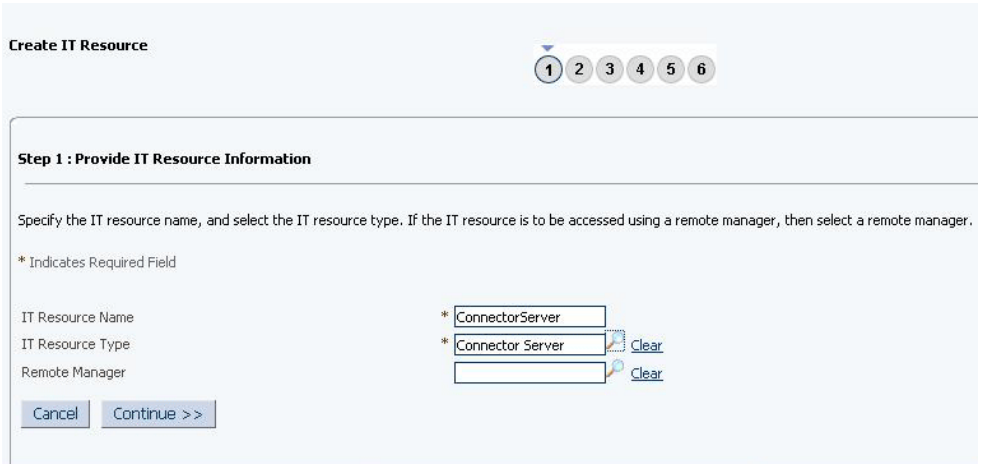
2.3.7 Creating the IT Resource for the Connector Server

> **Note:**
>
> Perform the procedure described in this section *only* if you have deployed the connector bundle remotely in a Connector Server.

To create the IT resource for the Connector Server:

1. If you are using Oracle Identity Manager release 11.1.1.*x,* then:
   a. Log in to the Administrative and User Console
   b. On the Welcome page, click **Advanced** in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Create IT Resource**.
2. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. Log in to Oracle Identity System Administration
   b. In the left pane, under Configuration, click **IT Resource.**
   c. In the Manage IT Resource page, click **Create IT Resource.**
3. On the Step 1: Provide IT Resource Information page, perform the following steps:
   - **IT Resource Name**: Enter a name for the IT resource.
   - **IT Resource Type**: Select **Connector Server** from the IT Resource Type list.
   - **Remote Manager**: Do not enter a value in this field.
4. Click **Continue**. Figure 2-3 shows the IT resource values added on the Create IT Resource page.

Figure 2-3 Step 1: Provide IT Resource Information



5. On the Step 2: Specify IT Resource Parameter Values page, specify values for the parameters of the IT resource and then click **Continue**. Figure 2-2 shows the Step 2: Specify IT Resource Parameter Values page.

Figure 2-4 Step 2: Specify IT Resource Parameter Values

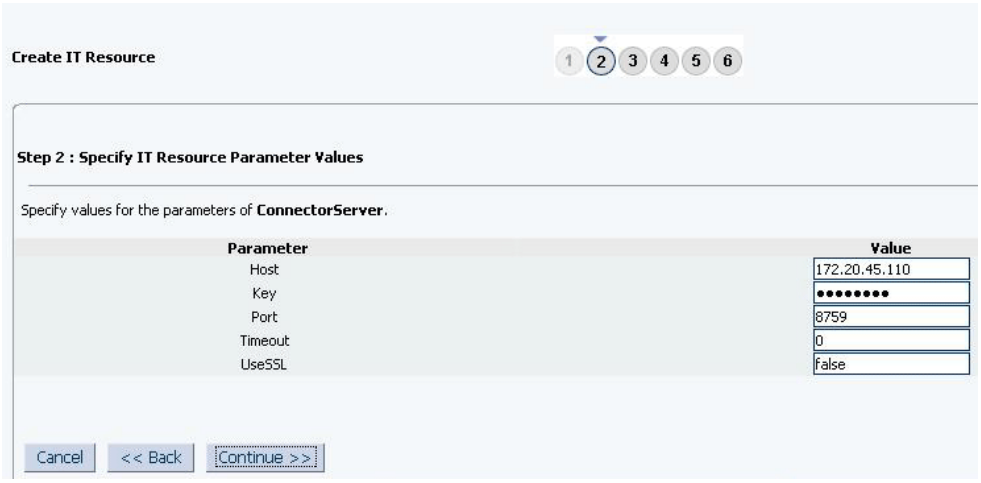


Figure 2-5 provides information about the parameters of the IT resource.

Table 2-4 Parameters of the IT Resource for the Connector Server

Parameter	Description
Host	Enter the host name or IP address of the computer hosting the connector server. Sample value: `RManager`
Key	Enter the key for the Java connector server.
Port	Enter the number of the port at which the connector server is listening. Default value: 8759

Table 2-4 (Cont.) Parameters of the IT Resource for the Connector Server

Parameter	Description
Timeout	Enter an integer value which specifies the number of milliseconds after which the connection between the connector server and Oracle Identity Manager times out. Sample value: `300`
UseSSL	Enter `true` to specify that you will configure SSL between Oracle Identity Manager and the Connector Server. Otherwise, enter `false`. Default value: `false` **Note:** It is recommended that you configure SSL to secure communication with the connector server. To configure SSL, run the connector server by using the /setKey [*key*] option. The value of this key must be specified as the value of the Key IT resource parameter of the connector server. To use SSL, you must set the value of connectorserver.usessl property to `true`, and then set the value of connectorserver.certifacatestorename to the certificate store name.

6. On the Step 3: Set Access Permission to IT Resource page, the `SYSTEM ADMINISTRATORS` group is displayed by default in the list of groups that have Read, Write, and Delete permissions on the IT resource that you are creating.

> **Note:**
>
> This step is optional.

If you want to assign groups to the IT resource and set access permissions for the groups, then:

a. Click **Assign Group**.

b. For the groups that you want to assign to the IT resource, select **Assign** and the access permissions that you want to set. For example, if you want to assign the `ALL USERS` group and set the Read and Write permissions to this group, then you must select the respective check boxes in the row, as well as the Assign check box, for this group.

c. Click **Assign**.

7. On the Step 3: Set Access Permission to IT Resource page, if you want to modify the access permissions of groups assigned to the IT resource, then:

> **Note:**
>
> - This step is optional.
> - You cannot modify the access permissions of the `SYSTEM ADMINISTRATORS` group. You can modify the access permissions of only other groups that you assign to the IT resource.

a. Click **Update Permissions**.

b. Depending on whether you want to set or remove specific access permissions for groups displayed on this page, select or deselect the corresponding check boxes.

c. Click **Update**.

8. On the Step 3: Set Access Permission to IT Resource page, if you want to unassign a group from the IT resource, then:

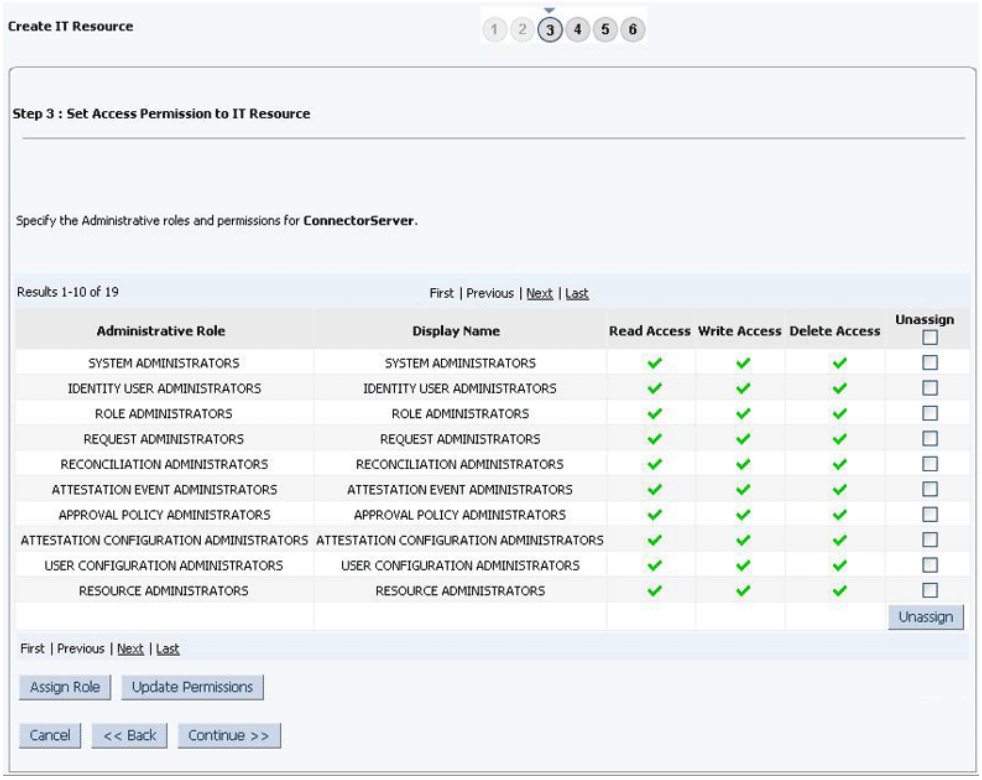
> **Note:**
>
> - This step is optional.
> - You cannot unassign the `SYSTEM ADMINISTRATORS` group. You can unassign only other groups that you assign to the IT resource.

a. Select the **Unassign** check box for the group that you want to unassign.

b. Click **Unassign**.

9. Click **Continue**. Figure 2-5 shows the Step 3: Set Access Permission to IT Resource page.

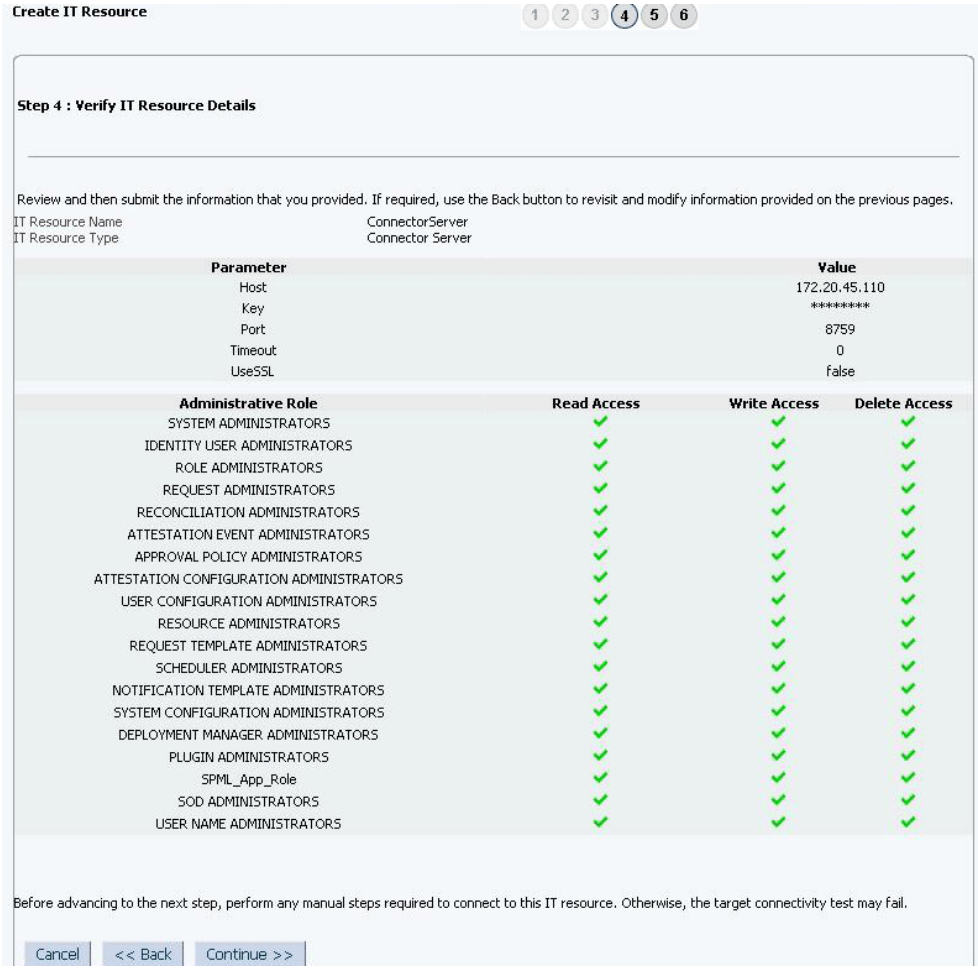
Figure 2-5 Step 3: Set Access Permission to IT Resource



10. On the Step 4: Verify IT Resource Details page, review the information that you provided on the first, second, and third pages. If you want to make changes in the data entered on any page, click **Back** to revisit the page and then make the required changes.

11. To proceed with the creation of the IT resource, click **Continue**. Figure 2-6 shows Step 4: Verify IT Resource Details page.

Figure 2-6 Step 4: Verify IT Resource Details

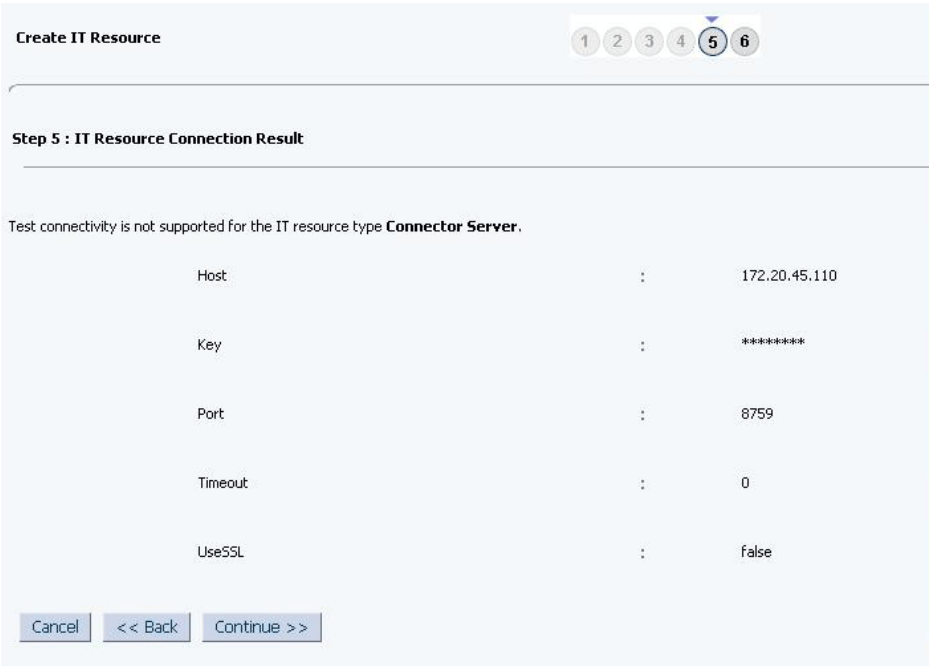


12. The Step 5: IT Resource Connection Result page displays the results of a connectivity test that is run using the IT resource information. If the test is successful, then click **Continue**. If the test fails, then you can perform one of the following steps:

    - Click **Back** to revisit the previous pages and then make corrections in the IT resource creation information.
    - Click **Cancel** to stop the procedure, and then begin from the first step onward.

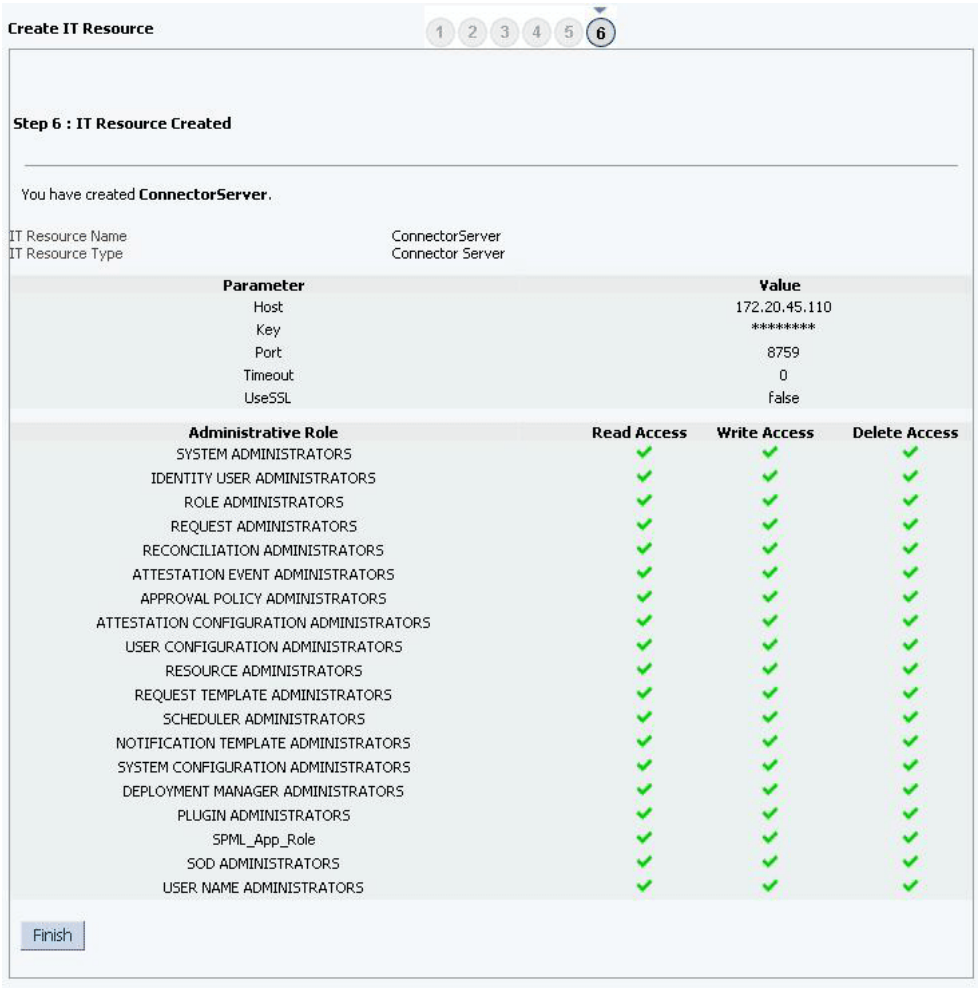
      Figure 2-7 shows the Step 5: IT Resource Connection Result page.

Figure 2-7 Step 5: IT Resource Connection Result



13. Click **Finish**. Figure 2-8 shows the IT Resource Created page.

Figure 2-8 Step 6: IT Resource Created



2.4 Upgrading the Connector

If you have already deployed an earlier release of this connector, then upgrade the connector to the current release 11.1.1.5.0.

The following sections discuss the procedure to upgrade the connector:

Note:

- Upgrade of the connector from release 9.0.4.*x* to 11.1.1.*x*. is supported.
- Before you perform the upgrade procedure, it is strongly recommended that you create a backup of the Oracle Identity Manager database. Refer to the database documentation for information about creating a backup.
- As a best practice, first perform the upgrade procedure in a test environment.

- Preupgrade Steps
- Upgrade Steps
- Postupgrade Steps

2.4.1 Preupgrade Steps

Perform the following preupgrade steps:

> **Note:**
>
> If you are using Oracle Identity Manager 11*g* Release 1 PS1 BP07 (11.1.1.5.7), then you must apply patch 16819090.
>
> To download a patch, sign in to My Oracle Support and search for the patch number on the Patches and Updates page at:
>
> `https://support.oracle.com/`

1. Perform a reconciliation run to fetch all latest updates to Oracle Identity Manager.
2. Define the source connector (an earlier release of the connector that must be upgraded) in Oracle Identity Manager. You define the source connector to update the Deployment Manager XML file with all customization changes made to the connector. See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.
3. If required, create the connector XML file for a clone of the source connector.
4. Disable all the scheduled jobs.

2.4.2 Upgrade Steps

Depending on the environment in which you are upgrading the connector, perform one of the following steps.

- Staging Environment

  Perform the upgrade procedure by using the wizard mode.

- Production Environment

  Perform the upgrade procedure by using the silent mode.

See Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the wizard and silent modes.

2.4.3 Postupgrade Steps

Postupgrade steps involve running the SQL script, running the Form Version Contol (FVC) utility, packaging the arapi***VERSION_NUM***.jar and log4j-1.2.14.jar files with the connector bundle jar, and so on.

1. Perform the postupgrade procedure documented in Managing Connector Lifecycle in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

2. Run the PostUpgradeScript.sql script as follows:
   a. Connect to the Oracle Identity Manager database by using the OIM User credentials.
   b. Run the PostUpgradeScript. This script is located in the Upgrade directory on the installation media.
3. Run the FVC utility to manage data changes on a form after an upgrade operation. To do so:
   a. In a text editor, open the fvc.properties file located in the *OIM_DC_HOME* directory and include the following entries:

      ```
      ResourceObject;BMCRO
      FormName;UD_BMC
      FromVersion;9.0.4.1
      ToVersion;SPECIFY_THE_VERSION_OF_FORM_THAT_IS_IN_THE_ACTIVE_STATUS_AFTER_THE_UPGRADE
      ```

   b. Run the FVC utility. This utility is copied into the following directory when you install the design console:

      For Microsoft Windows:

      OIM_DC_HOME/fvcutil.bat

      For UNIX:

      OIM_DC_HOME/fvcutil.sh

      When you run this utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, and the logger level and log file location.

      > **See Also:**
      >
      > Using the Form Version Control Utility in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about the FVC utility

4. Package the arapi***VERSION_NUM***.jar and log4j-1.2.14.jar files with the connector bundle jar as follows:
   a. Extract the contents of the org.identityconnectors.bmc-1.0.1115.jar file into a temporary directory.
   b. Create a directory named lib.
   c. Copy the arapi***VERSION_NUM***.jar and log4j-1.2.14.jar files to the lib directory.
   d. Update the connector bundle (org.identityconnectors.bmc-1.0.1115.jar) by running the following command:

      ```
      jar -cvfm org.identityconnectors.bmc-1.0.1115.jar META-INF/MANIFEST.MF *
      ```

> **Note:**
>
> While updating the connector bundle, ensure that META-INF \MANIFEST.MF file is unchanged.

5. Run the Oracle Identity Manager Upload JARs utility to post the new connector bundle (updated in Step 4) to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 4 as the value of the JAR type.

6. Configure the upgraded IT resource of the source connector. See Configuring the IT Resource for the Target System for information about configuring the IT resource.

7. Purge the cache to get the changes reflected in Oracle Identity Manager. See Purging Cache in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information on purging cache.

8. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:

   a. Log in to Oracle Identity System Administration.

   b. Create and activate a sandbox. See Creating and Activating a Sandbox.

   c. Create a new UI form to view the upgraded fields. See Creating a New UI Form for more information about creating a UI form.

   d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 8.8.c), and then save the application instance.

   e. Publish the sandbox. See Publishing a Sandbox.

After upgrading the connector, you can perform either full reconciliation or incremental reconciliation. This ensures that records created or modified since the last reconciliation run (the one that you performed in Preupgrade Steps) are fetched into

Oracle Identity Manager. From the next reconciliation run onward, the reconciliation engine automatically enters a value for the Latest Token attribute.

Before you perform lookup field synchronization, ensure to remove all preupgrade entries from the lookup definitions Oracle Identity Manager. After upgrade these values must be synchronized with the lookup fields in the target system.

See Configuring Reconciliation for more information about performing full or incremental reconciliation.

3
Using the Connector

You can use the BMC Remedy User Management connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.
This chapter is divided into the following sections:

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:

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

   See Scheduled Job for Lookup Field Synchronization for information about the attributes of the scheduled tasks for lookup field synchronization.

   See Configuring Scheduled Jobs for information about running scheduled tasks.

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

   See Reconciliation Scheduled Jobs for information about the attributes of this scheduled task.

   See Configuring Scheduled Jobs for information about running scheduled tasks.

After first-time reconciliation, depending on the mode in which you configure the connector, the Latest Token attribute is automatically set to the time stamp at which the reconciliation run completed.

> **See Also:**
>
> Configuring Scheduled Jobs for information about attributes of the scheduled job

From the next reconciliation run onward, only target system user records that are added or modified after the time stamp stored in the Latest Token attribute is considered for incremental reconciliation. These records are brought to Oracle Identity Manager when you configure and run the user reconciliation scheduled job.

3.2 Scheduled Job for Lookup Field Synchronization

The following scheduled jobs are used for lookup fields synchronization:

- BMC Company Lookup Reconciliation
- BMC Department Lookup Reconciliation
- BMC Organization Lookup Reconciliation
- BMC Primary Center Code Lookup Reconciliation
- BMC Region Lookup Reconciliation
- BMC Site Group Lookup Reconciliation
- BMC Site ID Lookup Reconciliation
- BMC Site Lookup Reconciliation
- BMC Support Group ID Lookup Reconciliation

You must specify values for the attributes of these scheduled jobs. Table 3-1 describes the attributes of these scheduled jobs. Configuring Scheduled Jobs describes the procedure to configure scheduled jobs.

Table 3-1 Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Code Key Attribute	Name of the connector or target system attribute that is used to populate the Code Key column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__UID__` **Note:** Do *not* change the value of this attribute.
Decode Attribute	Name of the connector or target system attribute that is used to populate the Decode column of the lookup definition (specified as the value of the Lookup Name attribute). Default value: `__NAME__` **Note:** Do *not* change the value of this attribute.
IT Resource Name	Enter the name of the IT resource for the target system installation from which you want to reconcile user records. Default value: `BMCRemedy Server`

Table 3-1 (Cont.) Attributes of the Scheduled Jobs for Lookup Field Synchronization

Attribute	Description
Lookup Name	Enter the name of the lookup definition in Oracle Identity Manager that must be populated with values fetched from the target system. Depending on the scheduled job that you are using, the default values are as follows: • For BMC Company Lookup Reconciliation: `Lookup.BMC.Company` • For BMC Department Lookup Reconciliation: `Lookup.BMC.Department` • For BMC Organization Lookup Reconciliation: `Lookup.BMC.Organization` • For BMC Primary Center Code Lookup Reconciliation: `Lookup.BMC.PrimaryCenterCode` • For BMC Region Lookup Reconciliation: `Lookup.BMC.Region` • For BMC Site Group Lookup Reconciliation: `Lookup.BMC.SiteGroup` • For BMC Site ID Lookup Reconciliation: `Lookup.BMC.SiteID` • For BMC Site Lookup Reconciliation: `Lookup.BMC.Site` • For BMC Support Group ID Lookup Reconciliation: `Lookup.BMC.SupportGroupID`
Object Type	Enter the type of object you want to reconcile. Depending on the scheduled job that you are running, the default value is one of the following: • For BMC Company Lookup Reconciliation: `COMPANY` • For BMC Department Lookup Reconciliation: `DEPARTMENT` • For BMC Organization Lookup Reconciliation: `ORGANIZATION` • For BMC Primary Center Code Lookup Reconciliation: `PRIMARY_CENTER_CODE` • For BMC Region Lookup Reconciliation: `REGION` • For BMC Site Group Lookup Reconciliation: `SITE_GROUP` • For BMC Site ID Lookup Reconciliation: `SITE_ID` • For BMC Site Lookup Reconciliation: `SITE` • For BMC Support Group ID Lookup Reconciliation: `SUPPORT_GROUP_ID`
Resource Object Name	Name of the resource object that is used for reconciliation. Default value: `BMCRO`

3.3 Configuring Reconciliation

You can configure the connector to specify the type of reconciliation and its schedule.

This section discusses the following topics related to configuring reconciliation:

- Performing Full Reconciliation
- Performing Limited Reconciliation
- Performing Batched Reconciliation
- Reconciliation Scheduled Jobs

3.3.1 Performing 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 no values are specified for the Latest Token and Filter attributes of the scheduled jobs for reconciling user records.
- Set the value of the Batch Start and Number of Batches attributes of the scheduled jobs for reconciling user records to `0`.

Note that the batch size can be set to any number of records to be fetched in a single batch. If the Batch Size attribute is set to the default value 0, then the value of the defaultBatchSize entry in the main configuration lookup definition (Lookup.BMC.Configuration or Lookup.BMC.Configuration.Trusted) is considered for batching.

At the end of the reconciliation run, the Latest Token attribute of the scheduled job for user record reconciliation is automatically set to the time stamp at which the run ended. 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 Performing 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.

You can perform limited reconciliation by creating filters for the reconciliation module. This connector provides a Filter attribute (a scheduled task attribute) that allows you to use any of the BMC Remedy User Management resource attributes to filter the target system records.

For detailed information about ICF Filters, see ICF Filter Syntax of *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

> **Note:**
>
> The __UID__ attribute name can only be used with the equalTo filter.

The following is also an example of a filter for an advanced search where you want to filter only those accounts whose last name is "Admin":

```
equals('1000000018','Admin')
```

In the preceding example, 1000000018 is the database ID of the LastName attribute in the target system.

While deploying the connector, follow the instructions in Configuring Scheduled Jobs to specify attribute values.

3.3.3 Performing Batched Reconciliation

This section discusses the Batch Size, Batch Start, and Number of Batches attributes of the scheduled jobs for target resource reconciliation (BMC User Target Reconciliation) and trusted source reconciliation (BMC User Trusted Reconciliation).

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. Depending on the number of records to be reconciled, this process may require a large amount of time. In addition, if the connection breaks during reconciliation, then the process would take longer to complete.

You can configure batched reconciliation to avoid such problems.

To configure batched reconciliation, specify values for the following attributes while performing the procedure described in the Scheduled Jobs for Reconciliation of User Records:

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

  If you set the value of this attribute to `0`, then the defaultbatchsize entry of the main configuration lookup (Lookup.BMC.Configuration or Lookup.BMC.Configuration.Trusted) is considered as the batch size for batched reconciliation. Any numeric value other than 0 takes precedence over the defaultbatchsize entry.
- Batch Start: Use this attribute to specify the record number from which batched reconciliation must begin.

  Set the value of this attribute to `0` to begin reconciliation from the first record in the target system. Similarly, set the value of this attribute to `1` to begin reconciliation from the second record in the target system and so on.
- Number of Batches: Use this attribute to specify the total number of batches that must be reconciled. The default value of this attribute is `0`. This implies that the connector fetches records in the maximum possible number of batches from the target system. In other words, all records starting from the record specified in the Batch Start attribute to the last record available in the target system is fetched. Any other valid number limits the number of batches to that specified value.

3.3.4 Reconciliation Scheduled Jobs

When you run the Connector Installer, the scheduled tasks corresponding to the following scheduled jobs are automatically created in Oracle Identity Manager:

- Scheduled Jobs for Reconciliation of User Records
- Scheduled Job for Reconciliation of Deleted Users Records

3.3.4.1 Scheduled Jobs for Reconciliation of User Records

Depending on whether you want to implement trusted source or target resource reconciliation, you must specify values for the attributes of one of the following user reconciliation scheduled jobs:

- BMC User Target Reconciliation

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

- BMC User Trusted Reconciliation

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

Table 3-2 describes the attributes of both scheduled jobs.

Table 3-2 Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
Batch Size	Enter the number of records that must be included in each batch fetched from the target system. Default value: `0` This attribute is used in conjunction with the Batch Start and Number of Batches attributes. All these attributes are discussed in Performing Batched Reconciliation.
Batch Start	Enter the number of the target system record from which a batched reconciliation run must begin. Default value: `0` This attribute is used in conjunction with the Batch Size and Number of Batches attributes. All these attributes are discussed in Performing Batched Reconciliation.

Filter	Expression for filtering records. Use the following syntax:
	`syntax = expression ( operator expression )*`
	`operator = 'and' | 'or'`
	`expression = ( 'not' )? filter`
	`filter = ('equalTo' | 'contains' | 'containsAllValues'`
	`| 'startsWith' | 'endsWith' | 'greaterThan' | 'greaterThanOrEqualTo'`
	`| 'lessThan' | 'lessThanOrEqualTo' ) '(' 'attributeName' ','`
	`attributeValue')'`
	`attributeValue = singleValue | multipleValues`
	`singleValue = 'value'`
	`multipleValues = '[' 'value_1' (',' 'value_n')* ']'`
	Default value: None

Incremental Recon Attribute	Database ID of the target system attribute that holds the date on which the user record was modified. Default value: 6 **Note:** Do *not* change the value of this attribute.
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile data. If you are running the BMC User Trusted Reconciliation scheduled job, then enter the name of the IT resource instance that you create for trusted source reconciliation in Configuring the IT Resource for the Target System. Sample value: `BMCRemedy Server`
Latest Token	This attribute holds the value of the target system attribute (6) that is specified as the value of the Incremental Recon Attribute attribute. The Latest Token attribute is used for internal purposes. By default, this value is empty. **Note:** Do *not* enter a value for this attribute. The reconciliation engine automatically enters a value in this attribute. Sample value: `1354753427000`

Table 3-2 (Cont.) Attributes of the Scheduled Jobs for Reconciliation of User Records

Attribute	Description
Number of Batches	Enter the number of batches that must be reconciled. Default value: `0` Sample value: `20` This attribute is used in conjunction with the Batch Start and Batch Size attributes. All these attributes are discussed in Performing Batched Reconciliation.
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. The default value of this attribute in the BMC User Target Reconciliation scheduled job is `BMCRO.` The default value of this attribute in the BMC User Trusted Reconciliation scheduled job is `BMCRO Trusted.`
Scheduled Task Name	Name of the scheduled task used for reconciliation. The default value of this attribute in the BMC User Target Reconciliation scheduled job is `BMC User Target Reconciliation.` The default value of this attribute in the BMC User Trusted Reconciliation scheduled job is `BMC User Trusted Reconciliation.`

3.3.4.2 Scheduled Job for Reconciliation of Deleted Users Records

Depending on whether you want to implement trusted source or target resource delete reconciliation, you must specify values for the attributes of one of the following scheduled jobs:

- BMC User Target Delete Reconciliation

  This scheduled job is used to reconcile data about deleted users in the target resource (account management) mode of the connector. During a reconciliation run, for each deleted user account on the target system, the BMC resource is revoked for the corresponding OIM User.

- BMC User Trusted Delete Reconciliation

  This scheduled job is used to reconcile data about deleted users in the trusted source (identity management) mode of the connector. During a reconciliation run, for each deleted target system user account, the corresponding OIM User is deleted.

Table 3-3 describes attributes of both scheduled jobs.

Table 3-3 Attributes of the Scheduled Job for Delete User Reconciliation

Attributes	Description
IT Resource Name	Name of the IT resource instance that the connector must use to reconcile user data. The default value of this attribute in the BMC User Target Delete Reconciliation scheduled job is `BMCRemedy Server`. The default value of this attribute in the BMC User Trusted Delete Reconciliation scheduled job is the name of the IT resource instance that you create for trusted source reconciliation in Configuring the IT Resource for the Target System.
Object Type	This attribute holds the type of object you want to reconcile. Default value: `User`
Resource Object Name	Enter the name of the resource object against which reconciliation runs must be performed. The default value of this attribute in the BMC User Target Delete Reconciliation scheduled job is `BMCRO`. The default value of this attribute in the BMC User Trusted Delete Reconciliation scheduled job is `BMCRO Trusted`.

3.4 Configuring Scheduled Jobs

Configure reconciliation jobs to perform reconciliation runs that check for new information on your target system periodically and replicates the data in Oracle Identity Governance.

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

See Scheduled Jobs for Lookup Field Synchronization and Reconciliation for the list of scheduled jobs that you can configure.

To configure a scheduled job:

1. If you are using Oracle Identity Manager release 11.1.1.*x*, then:
   a. Log in to the Administrative and User Console.
   b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
2. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then:
   a. Log in to Oracle Identity System Administration.
   b. In the left pane, under System Management, click **Scheduler.**
3. Search for and open the scheduled job as follows:
   a. 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.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.

4. 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.

> **See Also:**
>
> Creating Jobs in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

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

5. On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

> **Note:**
>
> - Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
> - Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.

6. 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 in Oracle Identity Manager Release 11.1.1.*x*

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, 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 Switching Between Request-Based Provisioning and Direct Provisioning.

The following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning

> **See Also:**
>
> Manually Completing a Task in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

- Direct Provisioning
- Request-Based Provisioning
- Switching Between Request-Based Provisioning and Direct Provisioning

> **Note:**
>
> The time required to complete a provisioning operation that you perform the first time by using this connector takes longer than usual.

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

5. 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.
6. On the Step 1: Select a Resource page, select **BMCRO** from the list and then click **Continue**.
7. On the Step 2: Verify Resource Selection page, click **Continue**.
8. On the Step 5: Provide Process Data for BMC User Details page, enter the details of the account that you want to create on the target system 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. Close the window displaying the "Provisioning has been initiated" message.
11. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.2 Request-Based Provisioning

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 this section 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.

- End User's Role in Request-Based Provisioning
- 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:

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:

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.

3.5.3 Switching Between Request-Based Provisioning and Direct Provisioning

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

If you have configured the connector for request-based provisioning, you can always switch to direct provisioning. Similarly, you can always switch back to request-based provisioning any time. This section discusses the following topics:

- Switching From Request-Based Provisioning to Direct Provisioning
- Switching From Direct Provisioning to Request-Based Provisioning

3.5.3.1 Switching From Request-Based Provisioning to Direct Provisioning

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

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.

3.5.3.2 Switching From Direct Provisioning to Request-Based Provisioning

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.

3.6 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

1. Log in to Oracle Identity Administrative and User console.
2. Create a user. See Creating Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance created for the BMC IT resource (in Creating an Application Instance), and then click **Checkout.**
5. Specify value for fields in the application form.

> **Note:**
>
> Ensure to select proper values for lookup type fields as there are a few dependent fields. Selecting a wrong value for such fields may result in provisioning failure.

6. Click **Ready to Submit.**
7. Click **Submit.**
8. If you want to provision entitlements, then:
   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

3.7 Uninstalling the Connector

If you want to uninstall the connector for any reason, see Uninstalling Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

4

Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.
This chapter discusses the following topics:

> **Note:**
>
> From Oracle Identity Manager Release 11.1.2 onward, lookup queries are not supported. See Managing Lookups in *Oracle Fusion Middleware Administering Oracle Identity Manager* for information about managing lookups by using the Form Designer in the Oracle Identity Manager System Administration console.

4.1 Adding New Attributes for Target Resource Reconciliation

> **Note:**
>
> You need not perform this procedure if you do not want to add new attributes for target resource reconciliation.

By default, the attributes listed in User Fields for Target Resource Reconciliation are mapped for target resource reconciliation between Oracle Identity Manager and the target system. If required, you can map additional attributes for target resource reconciliation as follows:

1. Determine the Database ID for the attribute that you want to add:
   a. Open the Remedy Administrator Console. Note that in the newer versions of the target system, this console is known as BMC Remedy Developer Studio.
   b. Expand **Servers.** If you are using the newer versions of the target system, expand **All Objects.**
   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. If you are using newer versions of the target system, the Database ID of the field is present either in the Outline window along with the field name or in the Properties window as the value of ID Property under Database.
2. Log in to the Oracle Identity Manager Design Console.
3. Add the new attribute on the OIM User process form as follows:
   a. Expand **Development Tools**.
   b. Double-click **Form Designer**.
   c. Search for and open the **UD_BMC** process form.
   d. Click **Create New Version**.
   e. In the **Label** field, enter the version name. For example, `version#1`.
   f. Click the Save icon.
   g. Select the current version created in Step e from the **Current Version** list.
   h. Click **Add** to create a new attribute, and provide the values for that attribute.

      For example, if you are adding the desk location attribute, then enter the following values in the **Additional Columns** tab:

Field	Value
Name	`UD_BMC_DESKLOCATION`
Variant Type	`String`
Length	`50`
Field Label	`DeskLocation`
Order	`26`

   i. Click the Save icon.
   j. Click **Make Version Active**.
4. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
   a. Log in to Oracle Identity System Administration.
   b. Create and active a sandbox. See Creating and Activating a Sandbox.
   c. Create a new UI form to view the newly added field along with the rest of the fields. See Creating a New UI Form for more information about creating a UI form.

d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 4.c), and then save the application instance.

e. Publish the sandbox. See Publishing a Sandbox.

5. Add the new attribute to the list of reconciliation fields in the resource object as follows:

   a. Expand **Resource Management.**

   b. Double-click **Resource Objects**.

   c. Search for and open the **BMCRO** resource object.

   d. On the **Object Reconciliation** tab, click **Add Field**, and then enter the following values:

      Field Name: `UD_BMC_DESKLOCATION`

      Field Type: `String`

   e. Click the Save icon and then close the dialog box.

6. Create a reconciliation field mapping for the new attribute in the process definition form as follows:

   a. Expand **Process Management.**

   b. Double-click **Process Definition**.

   c. Search for and open the **BMCPROCESS** process definition.

   d. On the **Reconciliation Field Mappings** tab, click **Add Field Map**, and then select the following values:

      Field Name: `DeskLocation`

      Field Type: `String`

      Process Data Field: `UD_BMC_DESKLOCATION`

   e. Click the Save icon.

   f. Click **Create Reconciliation Profile.** This copies changes made to the resource object into the MDS.

7. Create an entry for the attribute in the lookup definition for reconciliation as follows:

   a. Expand **Administration**.

   b. Double-click **Lookup Definition**.

   c. Search for and open the **Lookup.BMC.UM.ReconAttrMap** lookup definition.

   d. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the name of the attribute given in the resource object. The Decode value is the name or ID of the target system attribute.

      For example, enter `DeskLocation` in the **Code Key** field and then enter `1000000035` in the **Decode** field.

   e. Click the Save icon.

4.2 Adding New Attributes for Provisioning

> **Note:**
>
> - This section describes an optional procedure. You need not perform this procedure if you do not want to add new attributes for provisioning.
> - Before starting the following procedure, perform Steps 1 through 3 as described in Adding New Attributes for Target Resource Reconciliation. If these steps have been performed while adding new attributes for target resource reconciliation, then you need not repeat the steps.

By default, the attributes listed in User Fields for Target Resource Reconciliation are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning:

1. If you are using Oracle Identity Manager release 11.1.2.*x* or later, then all changes made to the Form Designer of the Design Console must be done in a new UI form as follows:
   a. Log in to Oracle Identity System Administration.
   b. Create and active a sandbox. See Creating and Activating a Sandbox.
   c. Create a new UI form to view the newly added field along with the rest of the fields. See Creating a New UI Form for more information about creating a UI form.
   d. Associate the newly created UI form with the application instance of your target system. To do so, open the existing application instance for your resource, from the Form field, select the form (created in Step 4.c of Adding New Attributes for Target Resource Reconciliation), and then save the application instance.
   e. Publish the sandbox. See Publishing a Sandbox.
2. Create an entry for the attribute in the lookup definition for provisioning as follows:
   a. Log in to the Oracle Identity Manager Design Console.
   b. Expand **Administration,** and then double-click **Lookup Definition.**
   c. Search for and open the **Lookup.BMC.UM.ProvAttrMap** lookup definition.
   d. Click **Add** and enter the **Code Key** and **Decode** values for the attribute. The Code Key value must be the value of the Field Label created in Step 3.3.h in Adding New Attributes for Target Resource Reconciliation. The Decode value is the name or ID of the attribute in the target system.

      For example, enter `DeskLocation` in the **Code Key** field and then enter `1000000035` in the Decode field.
   e. Click the Save icon.

> **Note:**
>
> Perform steps 3 through 5 only if both the condition are true:
>
> - You are using Oracle Identity Manager release 11.1.1.*x*.
> - You want to perform request-based provisioning.

3. Update the request dataset.

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

   a. In a text editor, open the xml/BMCRemedy-Datasets.xml file located on the installation media for editing.

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

      For example, if you added Address Number as an attribute on the process form, then enter the following line:

      ```
      <AttributeReference
      name = "DeskLocation"
      attr-ref = "DeskLocation"
      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_DESKLOCATION is the value in the Name column of the process form, then you must specify `DeskLocation` 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.

      - For the type attribute, enter the value that you entered in the Variant Type column of the process form.

      - For the widget attribute, enter the value that you entered in the Field Type column of the process form.

      - For the length attribute, enter the value that you entered in the Length column of the process form.

      - 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.

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

See *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

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

   See Importing Request Datasets for detailed information about the procedure.

4.2.1 Enabling Update of New Attributes for Provisioning

After you add an attribute for provisioning, you must enable update operations on the attribute. If you do not perform this procedure, then you will not be able to modify the value of the attribute after you set a value for it during the Create User provisioning operation.

To enable the update of a new attribute for provisioning a user:

1. Expand **Process Management.**
2. Double-click **Process Definition** and open the **BMCPROCESS** process definition.
3. In the process definition, add a new task for updating the field as follows:
   a. Click **Add** and enter the task name, for example, `DeskLocation Updated` and the task description.
   b. In the Task Properties section, select the **Conditional, Allow Cancellation while Pending,** and **Allow Multiple Instances** fields.
   c. Click on the Save icon.
4. On the Integration tab, click **Add,** and then click **Adapter.**
5. Select the **UpdateBMCUser** adapter, click **Save,** and then click **OK** in the message that is displayed.
6. To map the adapter variables listed in this table, select the adapter, click **Map,** and then specify the data given in the following table:

Variable Name	Data Type	Map To	Qualifier	Literal Value
processKeyInstance	Long	Process Data	Process Instance	NA
Adapter return value	Object	Response Code	NA	NA
objectType	String	Literal	String	User
attrFieldName	String	Literal	String	DeskLocation
itResourceFieldName	String	Literal	String	UD_BMC_IT_RESOURCE

7. Click the Save icon and then close the dialog box.

4.3 Configuring Validation of Data During Reconciliation and Provisioning

You can configure validation of reconciled and provisioned single-valued data according to your requirements. For example, you can validate data fetched from the First Name attribute to ensure that it does not contain the number sign (#). In addition, you can validate data entered in the First Name field on the process form so that the number sign (#) is not sent to the target system during provisioning operations.

To configure validation of data:

1. Write code that implements the required validation logic in a Java class.

   The following sample validation class checks if the value in the First Name attribute contains the number sign (#):

```
package org.identityconnectors.bmc.extension;
import java.util.*;
public class BMCValidator {

public boolean validate(HashMap hmUserDetails,
         HashMap hmEntitlementDetails, String field) {
            /*
         * You must write code to validate attributes. Parent
         * data values can be fetched by using hmUserDetails.get(field)
         * For child data values, loop through the
         * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
         * Depending on the outcome of the validation operation,
         * the code must return true or false.
         */
         /*
         * In this sample code, the value "false" is returned if the field
         * contains the number sign (#). Otherwise, the value "true" is
         * returned.
         */
            boolean valid=true;
            String sFirstName=(String) hmUserDetails.get(field);
            for(int i=0;i<sFirstName.length();i++){
              if (sFirstName.charAt(i) == '#'){
                    valid=false;
                    break;
              }
            }
            return valid;
        }
      } /* End */
```

2. Create a JAR file to hold the Java class.

3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 2 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. If you created the Java class for validating a process form field for reconciliation, then:
   a. Log in to the Design Console.
   b. Create a lookup definition named **Lookup.BMC.UM.ReconValidation.**
   c. In the Code Key column, enter the resource object field name that you want to validate For example, `Username`. In the Decode column, enter the class name. For example, `org.identityconnectors.bmc.extension.BMCValidator`.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.BMC.UM.Configuration** lookup definition.
   f. In the Code Key column, enter `Recon Validation Lookup`. In the Decode column, enter `Lookup.BMC.UM.ReconValidation`.
   g. Save the changes to the lookup definition.
5. If you created the Java class for validating a process form field for provisioning, then:
   a. Log in to the Design Console.
   b. Create a lookup definition by the name **Lookup.BMC.UM.ProvValidation.**
   c. In the Code Key column, enter the process form field name. In the Decode column, enter the class name.
   d. Save the changes to the lookup definition.
   e. Search for and open the **Lookup.BMC.UM.Configuration** lookup definition.
   f. In the Code Key column, enter `Provisioning Validation Lookup`. In the Decode column, enter `Lookup.BMC.UM.ProvValidation`.
   g. Save the changes to the lookup definition.
6. Purge the cache to get the changes reflected in Oracle Identity Manager. See *Oracle Fusion Middleware Administering Oracle Identity Manager* for information on purging cache.

4.4 Configuring Transformation of Data During Reconciliation

> **Note:**
>
> This section describes an optional procedure. Perform this procedure only if you want to configure transformation of data during reconciliation.

You can configure the transformation of reconciled single-valued data according to your requirements. For example, you can append the domain name with the first name.

To configure the transformation of data:

1. Write code that implements the required transformation logic in a Java class.

This transformation class must implement the transform method. The following sample transformation class modifies the Username attribute by using values fetched from the __NAME__ attribute of the target system:

```
pacakge oracle.iam.connectors.bmc;
import java.util.HashMap;
public class BMCTransformation {
public Object transform(HashMap hmUserDetails, HashMap
hmEntitlementDetails, String sField) throws ConnectorException {
      /*
      * You must write code to transform the attributes.
      * Parent data attribute values can be fetched by using
hmUserDetails.get("Field Name").
      * To fetch child data values, loop through the
      * ArrayList/Vector fetched by hmEntitlementDetails.get("Child Table")
      * Return the transformed attribute.
      */
        String sUserName = (String) hmUserDetails.get("__NAME__");
        return sUserName + "@example.com";
        }
}
```

2. Create a JAR file to hold the Java class.
3. Run the Oracle Identity Manager Upload JARs utility to post the JAR file created in Step 2 to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

For Microsoft Windows:

OIM_HOME/server/bin/UploadJars.bat

For UNIX:

OIM_HOME/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify 1 as the value of the JAR type.

4. Create a new lookup definition by the name **Lookup.BMC.UM.ReconTransformations** and then add the following entry:
   a. Log in to the Design Console.
   b. Expand **Administration,** and then double-click **Lookup Definition.**
   c. In the Code field, enter `Lookup.BMC.UM.ReconTransformations` as the name of the lookup definition.
   d. In the Field field, enter the name of the table column of the Oracle Identity Manager or user-created form or tab, from which the text field, lookup field, or box field will be accessible.
   e. Select the **Lookup Type** option.

f. On the Lookup Code Information tab, click **Add.**

g. In the **Code Key** column, enter the name of the attribute on which you want to apply the transformation. For example: `FirstName`.

h. In the **Decode** column, enter the name of the class file. For example: `oracle.iam.connectors.bmc.BMCTransformation`.

i. Save the lookup definition.

5. Purge the cache to get the changes reflected in Oracle Identity Manager. See *Oracle Fusion Middleware Administering Oracle Identity Manager* for information on purging cache.

4.5 Configuring the Connector for Multiple Installations of the Target System

You might want to configure the connector for multiple installations of the target system. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you can create copies of connector objects, such as the IT resource and resource object.

The decision to create a copy of a connector object is based on a requirement. For example, an IT resource can hold connection information for one target system installation. Therefore, it is mandatory to create a copy of the IT resource for each target system installation.

With some other connector objects, you do not need to create copies at all. For example, a single attribute-mapping lookup definition can be used for all installations of the target system.

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

1. Create a BMC connector bundle with a different version. To do so:

a. Extract the contents of the bundle/org.identityconnectors.bmc-1.0.1115.jar file on the installation media to a temporary directory.

b. In a text editor, open the MANIFEST.MF file located in the META-INF directory for editing.

c. Specify a new value for the ConnectorBundle-Version attribute. For example, specify `1.0.1117` as the new value.

d. Save and close the file.

e. Rename the connector bundle to reflect the new version. For example, org.identityconnectors.bmc-1.0.1117.jar.

2. Run the Oracle Identity Manager Upload JARs utility to upload the newly created JAR file (for example, org.identityconnectors.bmc-1.0.1117.jar file) to the database. This utility is copied into the following location when you install Oracle Identity Manager:

> **Note:**
>
> Before you use this utility, verify that the WL_HOME environment variable is set to the directory in which Oracle WebLogic Server is installed.

For Microsoft Windows:

OIM_HOME/server/bin/UploadJars.bat

For UNIX:

OIM_HOME/server/bin/UploadJars.sh

When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify `4` (ICFBundle) as the value of the JAR type.

3. Create a configuration lookup definition for this instance of the target system. For example, create a lookup definition by the name **Lookup.BMC.Configuration1.**
4. Add the following entries to this lookup definition and specify the corresponding values in the Decode column:
   - Connector Name
   - Bundle Version
   - User Configuration Lookup
   - Bundle Name

> **Note:**
>
> Ensure that the Decode value of Bundle Version is the latest version specified in Step 2. For example, `1.0.1117`. For all entries other than Bundle Version, you can specify the same values as those present in the Lookup.BMC.Configuration lookup definition.

5. Create an IT resource of the BMC IT Resource type. Ensure that the value of the Configuration Lookup parameter in this newly created IT resource contains the name of the lookup definition created in Step 4.
6. If you are using the connector server, then repeat steps 1 through 5 of this section with the following difference:

   While performing Step 2 of this procedure, instead of uploading the new created JAR file to Oracle Identity Manager database, copy it to the *CONNECTOR_SERVER_DIR*/bundles directory.

4.6 Configuring the Connector for Performing Reconciliation and Provisioning Operations on Custom Forms

By default, this connector provisions to and reconciles data from the CTM:People form. If you want to perform reconciliation and provisioning operations on custom forms, then you must modify the Configuration lookup definition and add two lookup entries as follows:

1. In the Design Console, expand **Administration,** and then double-click **Lookup Definition.**
2. Depending on whether you have configured the target system as a trusted source or target resource, search for and open the following lookup definition:
   - For trusted source reconciliation: **Lookup.BMC.Configuration.Trusted**
   - For target resource reconciliation: **Lookup.BMC.Configuration**
3. Click **Add.**
4. In the new row, enter values for the Code Key and Decode columns as follows:
   - **Code Key:** `userProvisioningFormName`
   - **Decode:** Enter the name of the custom form in the target system against which reconciliation and provisioning operations must be performed. Users are created, updated, deleted, and searched for from this form.

   > **Note:**
   >
   > If you do not specify a value in the Decode column, then reconciliation and provisioning operations are performed on the default form (CTM:People).

5. If you have configured your target system as a target resource, then click **Add** to add one more lookup entry to the **Lookup.BMC.Configuration** lookup definition.
6. In the new row, enter values for the Code Key and Decode columns as follows:
   - **Code Key:** `supportGrpAssocFormName`
   - **Decode:** Enter the custom form name in which association between a user and support group is created.

   > **Note:**
   >
   > If you do not specify a value in the Decode column, then the association between users and the support group is created in default form (CTM:Support Group Association).

7. Click **Save.**

4.7 Configuring the Connector for Performing Lookup Field Synchronization on Custom Forms

If you want to perform lookup field synchronization by specifying target system form names, then modify the value for the Object Type attribute of the scheduled job for lookup field synchronization in the following format:

OBJ_TYPE<FORM_NAME>

In this format, *OBJ_TYPE* is the type of object that is already present in the scheduled job. Suffix this object type with *FORM_NAME,* which is the name of the custom form on the target system against which lookup field synchronization runs must be performed.

Sample value: `COMPANY<COM:Company>`

Note:

- The custom form name that you specify in the *OBJ_TYPE<FORM_NAME>* format *must not* be the same as the one being used for performing provisioning operations. In other words, the custom form name *must not* be the same as the one that you specify for the userProvisioningFormName Code Key in the Configuration lookup definition.

  The custom form name in the *OBJ_TYPE<FORM_NAME>* format must contain only the form names against which you perform lookup field synchronization.
- If you do not specify the form name, then lookup field synchronization runs are performed against the default form associated with each lookup field.

See Also:

Scheduled Job for Lookup Field Synchronization for more information about the scheduled jobs for lookup field synchronization

5
Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected. You can use the testing utility, supplied with the connector package, to identify the cause of problems associated with connecting to the target system and performing basic operations on the target system.
The test-utility directory of connector installation media contains the following files:

- The example-config.groovy file is a sample configuration that can be used to set the connection properties of the target system and the connector.
- The README file contains instructions to configure and run the testing utility.
- The test-utility.jar file contains the class files used by the testing utility.

> **Note:**
>
> The testing utility does not support delete user operation.

To use the testing utility, perform the following steps:

1. Ensure JDK 1.6 is installed.
2. Extract the contents of the connector bundle into a temporary directory.
3. Locate and switch to the test-utility directory in the contents of the extracted zip file.

   The test-utility.jar and example-config.groovy files already exist in this directory.
4. Update the example-config.groovy file with the target system, connector bundle, and connector information.
5. Copy the following JAR files to the test-utility directory:
   - connector-framework.jar
   - connector-framework-internal.jar
   - groovy-all.jar

   > **Note:**
   >
   > These are files are delivered as part of the OIM EAR application, and they are located in the oim.ear/APP-INF/lib directory.
6. Copy the following third-party JAR files from the target system to the test-utility directory:
   - arapi***VERSION_NUM***.jar (replace *VERSION_NUM* with the release number of the target system that you are using)

For example, the arapi80_build001.jar file.

- log4j-1.2.14.jar

7. Run one of the following commands from the test-utility directory:

   - For UNIX:

     ```
     java -classpath ./test-utility.jar:./connector-framework.jar:./connector-
     framework-internal.jar:./groovy-all.jar:./arapi***VERSION_NUM***.jar:./
     log4j-1.2.14.jar oracle.iam.connectors.testutility.Main example-
     config.groovy | tee test.log
     ```

   - For Windows (assuming the current directory is c:\test-utility):

     ```
     java -classpath C:/test-utility/test-utility.jar;C:/test-utility/connector-
     framework.jar;C:/test-utility/connector-framework-internal.jar;C:/test-
     utility/groovy-all.jar;C:/test-utility/arapi***VERSION_NUM***.jar;C:/test-utility/
     log4j-1.2.14.jar oracle.iam.connectors.testutility.Main example-config.groovy
     ```

6
Known Issues and Workarounds

These are the known issues and workarounds associated with this release of the connector.

6.1 Lookup Field Synchronization Fails

> **Note:**
>
> This is an issue associated with Oracle Identity Manager. This issue is observed only in Oracle Identity Manager 11*g* release 1 BP07, Microsoft Windows 32-bit environment.

The following error is encountered when you perform lookup field synchronization:

java.lang.ClassCastException: java.lang.NoClassDefFoundError cannot be cast to org.identityconnectors.framework.common.objects.ConnectorObject

Workaround

Perform the following steps after you install the connector:

1. Run the Oracle Identity Manager Download JARs utility to download the connector bundle (org.identityconnectors.bmc-1.0.1115.jar) from the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/DownloadJars.bat

   For UNIX:

   OIM_HOME/server/bin/DownloadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being downloaded, and the location from which the JAR file must be downloaded. Specify `4` as the value of the JAR type.

> **See Also:**
>
> Migrating JARs and Resource Bundle in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility

2. Extract the contents of the org.identityconnectors.bmc-1.0.1115.jar file into a temporary directory.
3. Re-create the connector bundle (org.identityconnectors.bmc-1.0.1115.jar) without modifying the META-INF\MANIFEST.MF file by running the following command:

   ```
   jar -cvfm org.identityconnectors.bmc-1.0.1115.jar META-INF/MANIFEST.MF *
   ```

4. Run the Oracle Identity Manager Upload JARs utility to post the connector bundle (re-created in Step 3) to the Oracle Identity Manager database. This utility is copied into the following location when you install Oracle Identity Manager:

   > **Note:**
   >
   > Before you use this utility, verify that the `WL_HOME` environment variable is set to the directory in which Oracle WebLogic Server is installed.

   For Microsoft Windows:

   OIM_HOME/server/bin/UploadJars.bat

   For UNIX:

   OIM_HOME/server/bin/UploadJars.sh

   When you run the utility, you are prompted to enter the login credentials of the Oracle Identity Manager administrator, URL of the Oracle Identity Manager host computer, context factory value, type of JAR file being uploaded, and the location from which the JAR file is to be uploaded. Specify `4` as the value of the JAR type.

> **See Also:**
>
> Migrating JARs and Resource Bundle in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about the Upload JARs utility

A

Files and Directories On the Installation Media

These are the files and directories in the connector installation media that comprise the connector.
The contents of the connector installation media directory are described in Table A-1.

Table A-1 Files and Directories On the Installation Media

File in the Installation Media Directory	Description
bundle/org.identityconnectors.bmc-1.0.1115.jar	This JAR file contains the connector bundle.
configuration/BMC-CI.xml	This XML file contains configuration information that is used during the connector installation process.
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 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-utility/example-config.groovy	This file contains a sample configuration that you can modify to test basic provisioning operations.
test-utility/test-utility.jar	This JAR file contains the testing utility to conduct basic provisioning tests (create, update, and delete) on the connector.
upgrade/PostUpgradeScriptBMC.sql	This file is used during the connector upgrade procedure.
xml/BMC-ConnectorConfig.xml	This XML file contains definitions for the following connector components: • Resource objects • IT resource types • IT resource instance • Process forms • Process tasks and adapters • Process definition • Prepopulate rules • Lookup definitions • Reconciliation rules • Scheduled tasks
xml/BMCRemedy-Datasets.xml	This XML file contains dataset related definitions for the create and modify user provisioning operations. This file is used if you want to enable request-based provisioning. You import this XML file into Oracle Identity Manager by using the Deployment Manager. **Note:** This dataset must *not* be imported if you are using Oracle Identity Manager release 11.1.2 or later.

B

Scheduled Jobs for Lookup Field Synchronization and Reconciliation

These are all the scheduled jobs that you can configure for lookup field synchronization and reconciliation.

Table B-1 Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
BMC Company Lookup Reconciliation	This scheduled job is used to synchronize values of the company lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Department Lookup Reconciliation	This scheduled job is used to synchronize values of the department lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Organization Lookup Reconciliation	This scheduled job is used to synchronize values of the organization lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Primary Center Code Lookup Reconciliation	This scheduled job is used to synchronize values of the primary center code lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Region Lookup Reconciliation	This scheduled job is used to synchronize values of the region lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Site Group Lookup Reconciliation	This scheduled job is used to synchronize values of the site group lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Site ID Lookup Reconciliation	This scheduled job is used to synchronize values of the site ID lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Site Lookup Reconciliation	This scheduled job is used to synchronize values of the site lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC Support Group ID Lookup Reconciliation	This scheduled job is used to synchronize values of the support group ID lookup fields between Oracle Identity Manager and the target system. See Scheduled Job for Lookup Field Synchronization for information about this scheduled job.
BMC User Target Reconciliation	This scheduled job is used to fetch user data during target resource reconciliation. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of User Records.
BMC User Target Delete Reconciliation	This scheduled task is used to fetch data about deleted users during target resource reconciliation. During a reconciliation run, for each deleted user account on the target system, the BMC resource is revoked for the corresponding OIM User. For information about this scheduled task and its attributes, see Scheduled Job for Reconciliation of Deleted Users Records.

Table B-1 (Cont.) Scheduled Jobs for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
BMC User Trusted Reconciliation	This scheduled job is used to fetch user data during trusted source reconciliation. For information about this scheduled task and its attributes, see Scheduled Jobs for Reconciliation of User Records.
BMC User Trusted Delete Reconciliation	This scheduled job is used to fetch data about deleted users during trusted source reconciliation. During a reconciliation run, for each deleted target system account, the corresponding OIM User is deleted. For information about this scheduled task and its attributes, see Scheduled Job for Reconciliation of Deleted Users Records.