Oracle® Identity Manager

Connector Guide for IBM RACF Standard

Release 9.0.4

E10427-08

August 2018

ORACLE®

Oracle Identity Manager Connector Guide for IBM RACF Standard, Release 9.0.4

E10427-08

Primary Author: Alankrita Prakash

Contributing Authors: Gowri G. R, Debapriya Datta, Vagdevi Jayashankar, Devanshi Mohan

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 IBM RACF Standard.

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, see the Oracle Identity Manager documentation library.

For information about Oracle Identity Manager 9.0.4.*x* Connectors documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E10384_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.

Convention	Meaning
`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 IBM RACF Standard?

This chapter provides an overview of the updates made to the software and documentation for the IBM RACF Standard connector in release 9.0.4.12.

Note: Release 9.0.4.12 of the connector comes after release 9.0.4.3. Release numbers from 9.0.4.4 through 9.0.4.11 have not been used.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

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

Software Updates

The following sections discuss software updates:

- Software Updates in Release 9.0.4.1
- Software Updates in Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.12

Software Updates in Release 9.0.4.1

The following are software updates in release 9.0.4.1:

- In the "Postinstallation on the Target System" section on page 2-27, the procedure has been revised.
- In the "Importing the Connector XML Files" section on page 2-11, the `IsDebug` parameter has been removed from the list of IT resource parameters.
- In the "Performing Provisioning Operations" section on page 3-14, the names of the adapters have been modified.
- The `IsDebug` attribute has been removed from the scheduled tasks described in the following sections:

  - Lookup Field Synchronization
  - Submitjob User Reconciliation Scheduled Task
- In the "GetData User Reconciliation Scheduled Task" section on page 3-8, the `isTrusted` attribute has been added to the list of scheduled task attributes.

Software Updates in Release 9.0.4.2

The following are software updates in release 9.0.4.2:

- Using the Connector Installer
- Support for the Arabic Language
- Resolved Issues in Release 9.0.4.2

Using the Connector Installer

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

See "Installing the Connector on Oracle Identity Manager Release 9.1.0.x, Release 11.1.1, or Release 11.1.2" on page 2-6 for details.

Support for the Arabic Language

Arabic has been added to the list of supported languages.

See "Certified Languages" on page 1-3 in the connector guide for more information.

Resolved Issues in Release 9.0.4.2

The following are issues resolved in release 9.0.4.2:

Bug Number	Issue	Resolution
6610577	Group details were not reconciled during group lookup synchronization.	This issue has been resolved. The `LookupType` attribute has been added to the scheduled task for lookup field reconciliation. See "Lookup Field Synchronization" on page 3-2 for more information.
6724858	During a provisioning operation, special characters and spaces could not be entered in the `Department` field on the process form.	This issue has been resolved. The `Department` field can now accept special characters and spaces during provisioning operations.
6614438	During a Create User provisioning operation, the `RXPRNTDT` script was executed multiple times.	This issue has been resolved. The `RXPRNTDT` script is executed only once during a Create User provisioning operation.
6766603	The `RACFNonTrusted.xml` file was not correctly imported when you configured target resource reconciliation.	This issue has been resolved. The `RACFNonTrusted.xml` file is now correctly imported.

Software Updates in Release 9.0.4.3

The following are software updates in release 9.0.4.3:

- Resolved Issues in Release 9.0.4.3

Resolved Issues in Release 9.0.4.3

The following issue is resolved in release 9.0.4.3:

Bug Number	Issue	Resolution
7341339	While performing an Update User provisioning operation to modify the TSO parameter, the `size`, `unit`, and `maximum size` fields were not prepopulated.	This issue has been resolved. Error handlers have been added to check for null values for TSO parameters.

Software Updates in Release 9.0.4.12

The following are the software updates in release 9.0.4.12:

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

Support for New Oracle Identity Manager Release

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

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

Support for Request-Based Provisioning

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

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

Documentation-Specific Updates

The following sections provide documentation-specific updates:

- Documentation-Specific Updates Up to Release 9.0.4.2
- Documentation-Specific Updates in Release 9.0.4.3
- Documentation-Specific Updates in Release 9.0.4.12

Documentation-Specific Updates Up to Release 9.0.4.2

The following are the documentation-specific updates in release 9.0.4.2:

- Instructions in the "Configuring SSL" section on page 2-26 have been revised.
- In the "Verifying Deployment Requirements" section, changes have been made in the "Target System" row.

Documentation-Specific Updates in Release 9.0.4.3

The following is a documentation-specific update in release 9.0.4.3:

- There are no known issues in this release. In the "Known Issues" chapter, the following bug has been removed:

  Bug 7341339

  When you perform an Update User provisioning operation to modify the TSO parameter, the `size`, `unit`, and `maximum size` fields are not prepopulated. You must manually specify values for these fields.

- From this release onward:

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

The minimum certified release of JDK is release 1.4.2.

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

Documentation-Specific Updates in Release 9.0.4.12

The following documentation-specific updates have been made in revision "8" of release 9.0.4.12:

- The "Oracle Identity Manager" row of Table 1–1, " Certified Components" has been updated to include support for Oracle Identity Manager 11g R2, Oracle Identity Manager 11g R2 PS1, and Oracle Identity Manager 11g R2 PS2.
- The "Target system" row of Table 1–1, " Certified Components" has been updated to include support for IBM RACF v1.13.
- The "External code" row of Table 1–1, " Certified Components" has been updated to include support for IBM HOD version 11.0.
- In Section 5.2, "Troubleshooting", user id rules in the RACF target system have been added.
- In Section 5.2, "Troubleshooting", the default behavior of the RACF target system has been added.

The following documentation-specific update has been made in revision "7" of release 9.0.4.12:

In step 3 of Section 2.3.1.4, "Configuring Trusted Source Reconciliation," the path to locate and open the xml files have been updated.

The following documentation-specific update has been made in revision "6" of release 9.0.4.12:

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

1

About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. This guide discusses the procedure to deploy the connector that is used to integrate Oracle Identity Manager with IBM RACF Standard.

Note: The Oracle Identity Manager Advanced connector for IBM RACF provides an agent-based architecture for integrating IBM RACF with Oracle Identity Manager. For more information, see the guide for that connector.

This chapter contains the following sections:

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

At some places in this guide, IBM RACF Standard has been referred to as the *target system*.

1.1 Certified Components

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

Table 1–1 Certified Components

Component	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager Release 9.0.1 through 9.0.3.*x* ■ Oracle Identity Manager Release 9.1.0.1 and future releases in this release track **Note:** In this guide, **Oracle Identity Manager release 9.1.0.*x*** has been used to denote Oracle Identity Manager release 9.1.0.1 and future releases in the 9.1.0.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* release 1 (11.1.1.3.0) and future releases in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.1** has been used to denote Oracle Identity Manager release 11.1.1.3.0 and future releases in the 11.1.1.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* Release 1 PS1 (11.1.1.5.0) and future releases in this release track ■ Oracle Identity Manager 11*g* Release 1 PS2 (11.1.1.7.0) and future releases in this release track ■ Oracle Identity Manager 11*g* release 2 (11.1.2.0.0) and future releases in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.2** has been used to denote Oracle Identity Manager release 11.1.2.0.0 and future releases in the 11.1.2.*x* series that the connector will support. ■ Oracle Identity Manager 11*g* Release 2 PS1 (11.1.2.1.0) and future releases in this release track ■ Oracle Identity Manager 11*g* Release 2 PS2 (11.1.2.2.0) and future releases in this release track The connector does not support Oracle Identity Manager running on Oracle Application Server. For detailed information about certified components of Oracle Identity Manager, see the certification matrix on Oracle Technology Network at http://www.oracle.com/technetwork/documentation/oim1014-097544.html.
Target system	IBM RACF on z/OS V1.13

Table 1–1 (Cont.) Certified Components

Component	Requirement
External code	The following Host Access Class Library (HACL) class files obtained from IBM Host On-Demand (HOD) version 11.0: ■ hoddbg2.jar ■ hacp.jar ■ hasslite2.jar ■ habasen2.jar ■ WellKnownTrustedCAs.class ■ WellKnownTrustedCAs.p12 **Note**: My Oracle Support Patch 16034946 provides the latest version of the RACF connector and is certified with HOD 11.0.
Target system user account	Instructions to create an IBM RACF user account with the required privileges are given in Section 2.3.3, "Postinstallation on the Target System." You provide the credentials of this user account while configuring the IT resource. The procedure is described later in this guide. If the user account is not assigned the specified rights, then the "Authentication failure" message is displayed when Oracle Identity Manager tries to exchange data with the target system.
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x*, use JDK 1.4.2 or a later release in the 1.4.2 series. ■ For Oracle Identity Manager release 9.1.0.*x*, use JDK 1.5 or a later release in the 1.5 series. ■ For Oracle Identity Manager release 11.1.1, use JDK 1.6 update 18 or later, or JRockit JDK 1.6 update 17 or later.

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese Simplified
- Chinese Traditional
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

See Also: For information about supported special characters supported by Oracle Identity Manager, see one of the following guides:

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

  Oracle Identity Manager Globalization Guide

- For Oracle Identity Manager release 11.1.1:

  Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager

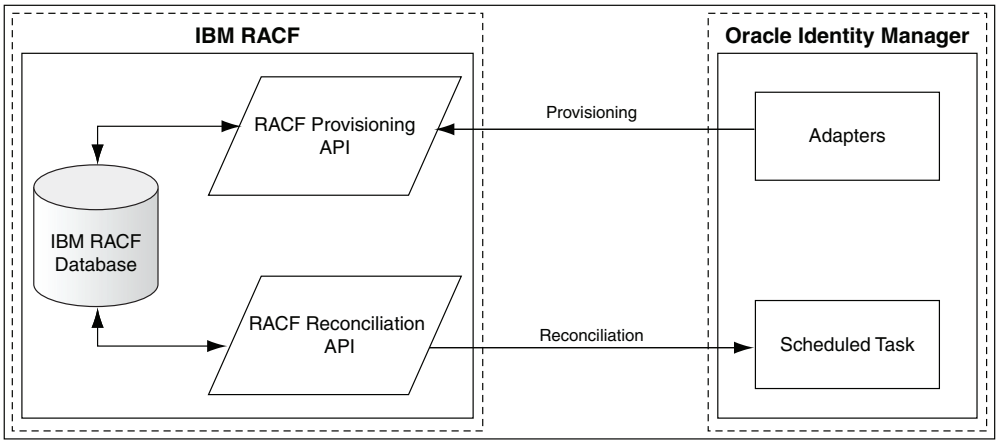
- For Oracle Identity Manager release 11.1.2:

  Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager

1.3 Connector Architecture

The architecture of the connector is the blueprint for the functionality of the connector. Figure 1–1 shows the architecture of the connector.

Figure 1–1 Architecture of the Connector



This figure shows the architecture of the connector. The description of the architecture is provided in this section.

****

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

Note: In Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

- Identity reconciliation

  In the identity reconciliation mode, IBM RACF Standard is used as the trusted source and users are directly created and modified on it.

  During reconciliation, a scheduled task establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager.

  Each record fetched from the target system is compared with existing OIM Users. If a match is found, then the update made to the record on the target system is copied to the OIM User attributes. If no match is found, then the target system record is used to create an OIM User.

- Account Management

  In the account management mode, IBM RACF Standard is used as a target resource. The connector enables the target resource reconciliation and provisioning operations. Through provisioning operations performed on Oracle Identity Manager, user accounts are created and updated on the target system for OIM Users. During reconciliation from the target resource, the IBM RACF Standard connector fetches into IBM RACF Standard data about user accounts that are created or modified on the target system. This data is used to add or modify resources allocated to OIM Users.

  During provisioning operations, adapters carry provisioning data submitted through the process form to the target system. APIs on the target system accept provisioning data from the adapters, carry out the required operation on the target system, and return the response from the target system to the adapters. The adapters return the response to Oracle Identity Manager.

  During reconciliation, a scheduled task establishes a connection with the target system and sends reconciliation criteria to the APIs. The APIs extract user records that match the reconciliation criteria and hand them over to the scheduled task, which brings the records to Oracle Identity Manager. The next step depends on the mode of connector configuration.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Support for Full Reconciliation"
- Section 1.4.2, "Support for Target Resource and Trusted Source Reconciliation"
- Section 1.4.3, "Support for Limited Reconciliation"
- Section 1.4.4, "Support for Batched Reconciliation"

1.4.1 Support for Full 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.

See Section 3.3.1, "Full Reconciliation" for more information.

1.4.2 Support for Target Resource and Trusted Source Reconciliation

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

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

1.4.3 Support for Limited Reconciliation

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

- Filter Auditor Privilege (Y/N)
- Filter Default Group
- Filter Group Access Privilege (Y/N)
- Filter Name
- Filter Operations Privilege (Y/N)
- Filter Owner
- Filter Special Privilege (Y/N)
- Filter User Id
- Filter Type (AND/OR)

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

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

1.4.4 Support for Batched Reconciliation

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

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

1.5 Lookup Definitions Used During Reconciliation and Provisioning

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

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

1.5.1 Lookup Definitions Synchronized with the Target System

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

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

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

- Lookup.RACF.Groups
- Lookup.RACF.Accounts
- Lookup.RACF.Procedures

1.5.2 Other Lookup Definitions

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

Table 1–2 Other Lookup Definitions

Lookup Definition	Description of Values	Method to Specify Values for the Lookup Definition
Connect	This lookup definition holds information about the authority that you can select for a target system account that you create through Oracle Identity Manager.	This lookup definition is preconfigured. You can add or modify entries in this lookup definition. See one of the following guides for more information about modifying entries in a lookup definition: ■ For Oracle Identity Manager release 9.0.1. through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide* ■ For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager* ■ For Oracle Identity Manager release 11.1.2: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

1.6 Connector Objects Used During Target Resource Reconciliation and Provisioning

See Also: One of the following guides for conceptual information about reconciliation:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.2: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

- Section 1.6.1, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.2, "Group Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.3, "TSO Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.6.4, "Reconciliation Rule for Target Resource Reconciliation"
- Section 1.6.5, "Reconciliation Action Rules for Target Resource Reconciliation"
- Section 1.6.6, "Provisioning Functions"

1.6.1 User Attributes for Target Resource Reconciliation and Provisioning

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

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

Process Form Field	Target System Field	Description
userid	USBD_NAME	User ID that is determined from the user profile name
owner	USBD_OWNER_ID	User ID or group that owns the profile
name	USBD_PROGRAMMER	Display name associated with the user ID
default group	USBD_DEFGRP_ID	Default group associated with the user
operations	USBD_OPER	Specifies whether the user has the Operations privilege
auditor	USBD_AUDITOR	Specifies whether the user has the Auditor privilege
special	USBD_SPECIAL	Specifies whether the user has the Special privilege
grp access	USBD_GRPACC	Specifies whether the user has the GRPACC privilege
department	USWRK_DEPARTMENT	Department name

1.6.2 Group Attributes for Target Resource Reconciliation and Provisioning

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

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

Process Form Field	Target System Support Group Attribute	Description
Group	USCON_GRP_ID	Name of the group name with which the user is associated
Revoke Date	USCON_REVOKE_DATE	Date on which the user's association with the group ends
Authorisation	GPMEM_AUTH	Authorization privilege

1.6.3 TSO Attributes for Target Resource Reconciliation and Provisioning

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

Table 1–5 TSO Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	Target System TSO Attribute	Description
Account Number	USTSO_ACCOUNT	Default account number
Procedure	USTSO_LOGON_PROC	Default procedure name
Size	USTSO_SIZE	Default memory space allocated to the user in TSO
Unit	USTSO_UNIT	Default unit of measurement of memory size
Maximum Size	USTSO_MAXIMUM_SIZE	Default maximum memory space that can be allocated to the user in TSO

1.6.4 Reconciliation Rule for Target Resource Reconciliation

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

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.2: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process-matching rule:

Rule Name: reconcile RACF data

Rule Element: User Login Equals userid

In this rule:

- User Login is one of the following:
  - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x*:

    User ID attribute on the Xellerate User form.
  - For Oracle Identity Manager release 9.1.0.*x* or release 11.1.1:

    User ID attribute on the OIM User form.
  - For Oracle Identity Manager release 11.1.2:

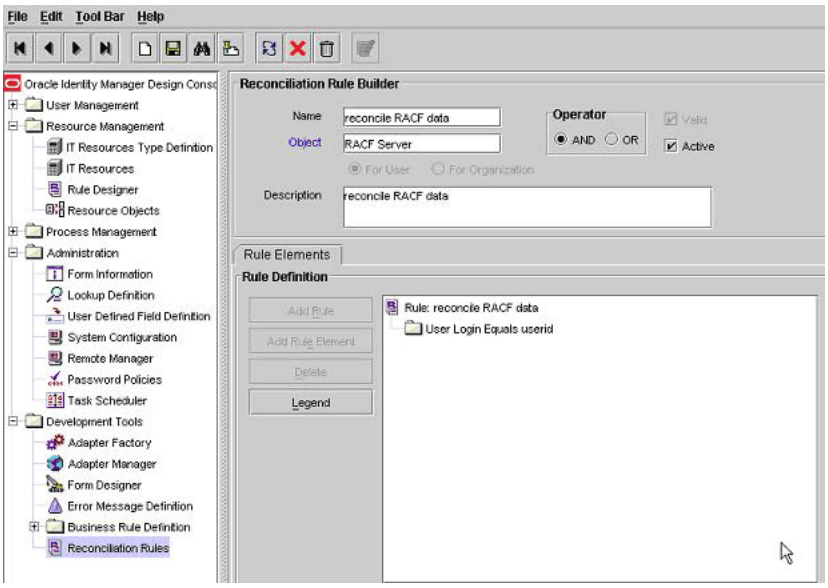
- userid is the USBD_NAME attribute of the target system.

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

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools.**
3. Double-click **Reconciliation Rules.**
4. Search for and open **reconcile RACF data.** Figure 1–2 shows this reconciliation rule.

Figure 1–2 Reconciliation Rule for Target Resource Reconciliation



This screenshot shows the Reconciliation Rule Builder form. The rule definition is displayed on the Rule Elements tab.

****

1.6.5 Reconciliation Action Rules for Target Resource Reconciliation

Table 1–6 lists the action rules for target resource reconciliation.

Table 1–6 Action Rules for Target Resource Reconciliation

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

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

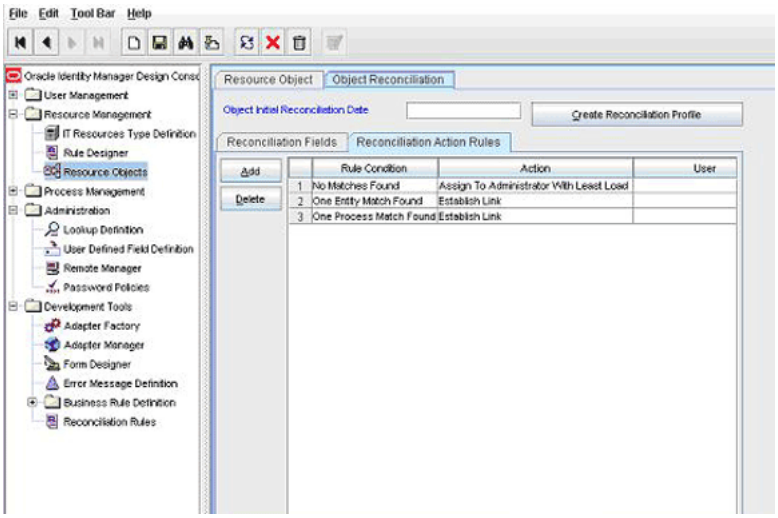
- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.2: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*

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

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

2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **RACF User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–3 shows the reconciliation action rule for target resource reconciliation.

Figure 1–3 Reconciliation Action Rules for Target Resource Reconciliation



This screenshot shows the Resource Objects form. The action rules are displayed on the Reconciliation Action Rules tab.

****

1.6.6 Provisioning Functions

Table 1–7 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 1–7 Provisioning Functions

Function	Adapter
Create a RACF User	adpCREATENEWRACFUSER
Delete a RACF User	adpRACFUSERDELETE
Name Updated	adpUPDATERACFUSERATTRIBUTE
Password Updated	adpSETRACFUSERPASSWORD
Department Updated	adpUPDATERACFUSERATTRIBUTE
Default Group Updated	adpUPDATERACFUSERATTRIBUTE
Installation data Updated	adpUPDATERACFUSERATTRIBUTE
Operations Updated	adpRACFUPDATEPRIVILEDGE
Special Updated	adpRACFUPDATEPRIVILEDGE
Auditor Updated	adpRACFUPDATEPRIVILEDGE

Table 1–7 (Cont.) Provisioning Functions

Function	Adapter
Group Access Updated	adpRACFUPDATEPRIVILEDGE
Owner Updated	adpUPDATERACFUSERATTRIBUTE
Enable a RACF User	adpRACFUSERENABLE
Disable a RACF User	adpRACFUSERDISABLE
Connect Group	adpCONNECTTOGROUP
Disconnect Group	adpDISCONNECTFROMGROUP
Add TSO to a User	adpADDTSOTORACFUSER
Remove TSO	adpREMOVETSO

1.7 Connector Objects Used During Trusted Source Reconciliation

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

- Section 1.7.1, "User Attributes for Trusted Source Reconciliation"
- Section 1.7.2, "Reconciliation Rule for Trusted Source Reconciliation"
- Section 1.7.3, "Reconciliation Action Rules for Trusted Source Reconciliation"

1.7.1 User Attributes for Trusted Source Reconciliation

Table 1–8 lists user attributes for trusted source reconciliation.

Table 1–8 User Attributes for Trusted Source Reconciliation

OIM User Form Field	Target System Attribute	Description
User ID	USBD_NAME	Common name
First Name	FName	First name
Last Name	LName	Last name
Employee Type	NA	Default value: `Consultant`
User Type	NA	Default value: `End-User Administrator`
Organization	NA	Default value: `Xellerate Users`

1.7.2 Reconciliation Rule for Trusted Source Reconciliation

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

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Connector Concepts*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.2: *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*

The following is the process matching rule:

Rule name: RACF Trusted Rule

Rule element: User Login Equals userid

In this rule element:

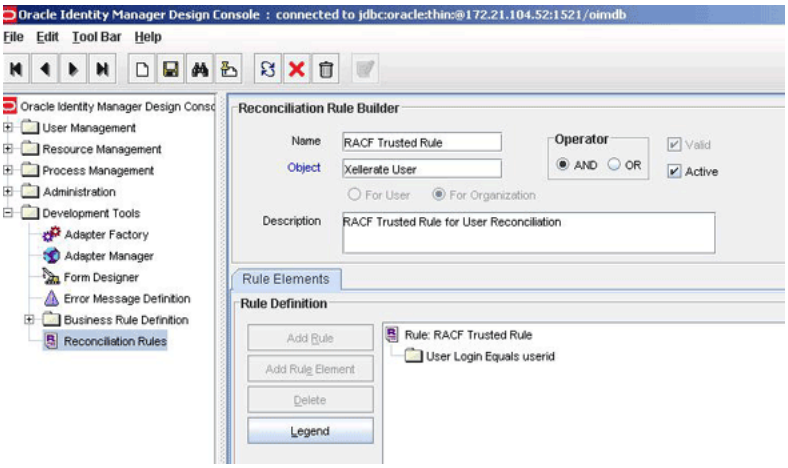
- User Login is the User ID field on the OIM User form.
- userid is the USBD_NAME field of RACF Standard.

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

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Development Tools**.
3. Double-click **Reconciliation Rules**.
4. Search for **RACF Trusted Rule**. Figure 1–4 shows the reconciliation rule for trusted source reconciliation.

Figure 1–4 Reconciliation Rule for Trusted Source Reconciliation



This screenshot shows the Reconciliation Rule Builder form. The rule definition is displayed on the Rule Elements tab.

****

1.7.3 Reconciliation Action Rules for Trusted Source Reconciliation

Table 1–9 lists the action rules for target source reconciliation.

Table 1–9 Action Rules for Target Source Reconciliation

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

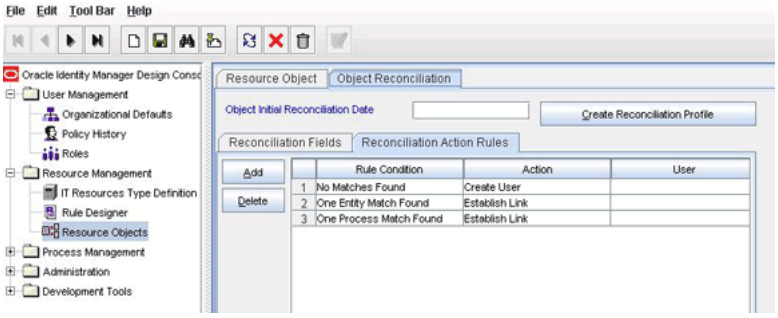
Note: No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see one of the following guides:

- For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *Oracle Identity Manager Design Console Guide*
- For Oracle Identity Manager release 11.1.1: *Oracle Fusion Middleware Developer's Guide for Oracle Identity Manager*
- For Oracle Identity Manager release 11.1.2: *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*

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

1. Log in to the Oracle Identity Manager Design Console.
2. Expand **Resource Management**.
3. Double-click **Resource Objects**.
4. Search for and open the **Xellerate User** resource object.
5. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rules for trusted source reconciliation.

Figure 1–5 Reconciliation Action Rules for Trusted Source Reconciliation



This screenshot shows the Resource Objects form. The action rules are displayed on the Reconciliation Action Rules tab.

****

1.8 Roadmap for Deploying and Using the Connector

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

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

- Chapter 3, "Using the Connector" describes guidelines on using the connector and the procedure to configure reconciliation runs and perform provisioning operations.
- Chapter 4, "Extending the Functionality of the Connector" describes procedures that you can perform if you want to extend the functionality of the connector.
- Chapter 5, "Testing and Troubleshooting" describes the procedure to use the connector testing utility for testing the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2

Deploying the Connector

To deploy the connector, perform the procedures described in the following sections:

- Section 2.1, "Preinstallation"
- Section 2.2, "Installation"
- Section 2.3, "Postinstallation"

2.1 Preinstallation

This section is divided into the following topics:

- Section 2.1.1, "Preinstallation on Oracle Identity Manager"
- Section 2.1.2, "Preinstallation on the Target System"

2.1.1 Preinstallation on Oracle Identity Manager

This section contains the following topics:

- Section 2.1.1.1, "Files and Directories on the Installation Media"
- Section 2.1.1.2, "Determining the Release Number of the Connector"
- Section 2.1.1.3, "Using External Code Files"

2.1.1.1 Files and Directories on the Installation Media

Table 2–1 describes the files and directories on the installation media.

Table 2–1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
configuration/IBM RACF Standard-CI.xml	This XML file contains configuration information that is used during connector installation.
Files in the dataset directory	These XML files specify the information to be submitted by the requester during a request-based provisioning operation.
lib/xlUtilHostAccess.jar	This JAR file contains the class files that are required for provisioning. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/JavaTasks ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database ■ For Oracle Identity Manager release 11.1.2: Oracle Identity Manager database
lib/xlReconRACF.jar	This JAR file contains the class files that are required for reconciliation. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/ScheduleTask ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database ■ For Oracle Identity Manager release 11.1.2: Oracle Identity Manager database
ext/CustomizedCAs.jar	This file is used to set up an SSL connection between Oracle Identity Manager and the IBM Mainframe server.
config/InitialLoginSequence.txt	This file contains the login sequence that the connector uses to connect to the IBM Mainframe server. The login sequence contains the sequence of values to be provided to the Telnet session between the connector and the IBM Mainframe server. These values are required to navigate through the various screens that are part of the TSO login process before reaching the `READY` prompt on the mainframe target server. The values in this file are supplied in the form of variables that hold IT resource values and literals. This machine-dependent file must be altered after deployment.
config/InputFields.txt	This file contains values for the connection parameters that are required to connect to the IBM Mainframe server. This file is used with the testing utility.
config/LogOutSequence.txt	This file contains the logoff sequence that the connector uses to log off from the IBM Mainframe server. The logoff sequence contains the sequence of values to be provided to the Telnet session between the connector and the IBM Mainframe server. These values are required to navigate through the various screens that are part of the TSO logoff process from the `READY` prompt on the mainframe target server. The values in this file are supplied in the form of variables that hold IT resource values and literals. This machine-dependent file must be altered after deployment.
scripts/DATAEXTT	This file uses the decrypted copy of the IBM RACF database to extract user-related records required for reconciliation to temporary files. It is a member of a procedure library on the IBM Mainframe server.

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

File in the Installation Media Directory	Description
scripts/DATAUNLD	This file merges the data from the SYSTMDAT and JCLSRC files to a temporary file to submit a background job. This background job prepares a decrypted copy of the IBM RACF database and then calls the individual REXX code scripts to format the data.
scripts/JCLSRC	This file is used to submit the background job for use in reconciliation. It is a member of a procedure library on the IBM Mainframe server. A procedure library is a partitioned dataset containing member files.
scripts/JOBSTAT	This file determines the status of a background job used for reconciliation. It is a member of a procedure library on the IBM Mainframe server.
scripts/RECNLKUP	This file provides lookup fields data. It is a member of a procedure library on the IBM Mainframe server.
scripts/RXDIFFER	This file provides differences between the old and new database images. It is a member of a procedure library on the IBM Mainframe server.
scripts/RXDPTADD	This file copies the user's department data from a temporary file and adds this information to the user's basic data. It is a member of a procedure library on the IBM Mainframe server.
scripts/RXGRPADD	This file copies the user's group privilege data from a temporary file and adds this information to the user's basic data. It is a member of a procedure library on the IBM Mainframe server.
scripts/RXPRNTDT	This file carries user reconciliation data from the IBM Mainframe to Oracle Identity Manager. It is a member of a procedure library on the IBM Mainframe server.
scripts/RXPRVADD	This file copies the user's connect privilege data from a temporary file and adds this information to the user's basic data. It is a member of a procedure library on the IBM Mainframe server.
scripts/RXTSOADD	This file copies the user's TSO data from a temporary file and adds this information to the user's basic data. It is a member of a procedure library on the IBM Mainframe server.
scripts/SYSTMDAT	This file is used to provide job configuration parameters to the mainframe system.
Files in the resources directory	Each of these resource bundles contains language-specific information that is used by the connector. During connector installation, this file is copied to the following location: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/connectorResources ■ For Oracle Identity Manager release 11.1.1: Oracle Identity Manager database ■ For Oracle Identity Manager release 11.1.2: Oracle Identity Manager database **Note:** A resource bundle is a file containing localized versions of the text strings that include GUI element labels and messages.
test/config/config.properties	This testing utility file holds the input data that you provide for each test.
test/config/log.properties	This testing utility file holds log data that is generated after each test.

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

File in the Installation Media Directory	Description
test/scripts/RACF.sh test/scripts/RACF.bat	This file is used to run the testing utility.
xml/RACFnonTrusted.xml	These XML files contain definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Resource object form ■ Process definition ■ Process tasks ■ Connector tasks
xml/RACFTrusted.xml	This XML file contains the configuration for the Xellerate User (OIM User). You must import this file only if you plan to use the connector in trusted source reconciliation mode.

Note: The files in the test directory are used only to run tests on the connector.

2.1.1.2 Determining the Release Number of the Connector

Note: If you are using Oracle Identity Manager release 9.1.0.*x*, then the procedure described in this section is optional.

If you are using Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2, then skip this section.

You might have a deployment of an earlier release of the connector. While deploying the latest release, you might want to know the release number of the earlier release. To determine the release number of the connector that has already been deployed:

1. In a temporary directory, extract the contents of the following JAR file:

   OIM_HOME/xellerate/JavaTasks/xlUtilHostAccess.jar

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

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

2.1.1.3 Using External Code Files

The procedure to copy the external code files involves the following steps:

1. Create a JAR file containing the WellKnownTrustedCAs.class and `WellKnownTrusted.p12` files. These files are available as part of the HOD installation in the following directory (assuming HOD is installed in the <../IBM> directory):

   <IBM/HostOnDemand/HOD>

   You can use the following command to create the JAR file:

```
jar -cvf  WellKnownTrustedCertificatesCAs.jar  WellKnownTrustedCAs.class
WellKnownTrusted.p12
```

2. Copy the JAR file created in Step 1 along with the external JAR files (hoddbg2.jar, hacp.jar, habasen2.jar, and hasslite2.jar) available in the HOD installation directory (<.IBM/HostOnDemand/HOD>) to the following directory of the Oracle Identity Manager installation:

   Note: In an Oracle Identity Manager cluster, copy this JAR file into the ThirdParty directory on each node of the cluster.

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

     OIM_HOME/xellerate/ThirdParty

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ThirdParty

   - For Oracle Identity Manager release 11.1.2:

     OIM_HOME/server/ThirdParty

3. Copy the InitialLoginSequence.txt, LogOutSequence.txt, and InputFields.txt files to the following directory after making changes (if required) according to the target configuration:

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

     OIM_HOME/xellerate/ThirdParty

   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ThirdParty

   - For Oracle Identity Manager release 11.1.2:

     OIM_HOME/server/ThirdParty

2.1.2 Preinstallation on the Target System

To create a target system user account for connector operations:

1. Create a user on the IBM Mainframe server with TSO access using an existing user account to which the `Special` attribute has been assigned. To do so, run the following REX program:

```
PROC 0
   ADDUSER (User Id) OWNER(Group Name) +
      NAME(' (User Id) - User Name') +
      TSO(PROC(TSO procedure Name) +
         ACCTNUM(Account Name) +
         SIZE(2096) +
         UNIT(2096) +
      )
      RDEFINE ACCTNUM Account Name UACC(NONE)
      PERMIT Account Name CLASS(ACCTNUM) ID((User Id)) ACCESS(READ)
      PERMIT TSO procedure Name CLASS(TSOPROC) ID((User Id)) ACCESS(READ)
      ADDSD '(User Id).*' UACC(NONE)
      PE '(User Id).*' ACCESS(ALTER) ID((User Id))
      CO (User Id) GROUP(Group Name)
      ALU (User Id) DFLTGRP(Group Name)
      ALU (User Id) PASS(Password)
```

```
SETR RACLIST(ACCTNUM) REFRESH
SETR RACLIST(TSOPROC) REFRESH
```

2. Provide the user with the `Special` attributes.
   a. Log on to TSO on the IBM Mainframe server using the user account that you use to create the mainframe user.
   b. At the `READY` prompt, enter the following command:

      ```
      Altuser NewUserIDCreated Special
      ```

3. Enter the following RACF commands at the READY prompt to provide the mainframe user with the ALTER permission on the directory that is to store the RACF scripts:

   ```
   ADDSD  RACF_Source UACC(NONE)
   PERMIT RACF_Source ACCESS(ALTER) ID(new_mainframe_userid)
   SETROPTS GENERIC(DATASET) REFRESH
   ```

4. Set `Msgid` to `ON` for the mainframe user as follows:
   a. Log on to TSO on the IBM Mainframe server using the mainframe user account that you create.
   b. At the READY prompt, enter the following command:

      ```
      profile msgid
      ```

2.2 Installation

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

- Section 2.2.1, "Installing the Connector on Oracle Identity Manager Release 9.1.0.x, Release 11.1.1, or Release 11.1.2"
- Section 2.2.2, "Installing the Connector on Oracle Identity Manager Release 9.0.1 Through 9.0.3.x"

2.2.1 Installing the Connector on Oracle Identity Manager Release 9.1.0.*x*, Release 11.1.1, or Release 11.1.2

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

Installing the connector on Oracle Identity Manager release 9.1.0.*x*, release 11.1.1, or release 11.1.2 involves the following procedures:

- Section 2.2.1.1, "Running the Connector Installer"
- Section 2.2.1.2, "Configuring the IT Resource"

2.2.1.1 Running the Connector Installer

To run the Connector Installer:

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

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

- For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/ConnectorDefaultDirectory
- For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/ConnectorDefaultDirectory
- For Oracle Identity Manager release 11.1.2: *OIM_HOME*/server/ConnectorDefaultDirectory

2. Log in to the Administrative and User Console by using the user account described in the "Creating the User Account for Installing Connectors" section of the following guide:
   - For Oracle Identity Manager release 9.1.0.*x*:

     Oracle Identity Manager Administrative and User Console Guide
   - For Oracle Identity Manager release 11.1.1:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager
   - For Oracle Identity Manager release 11.1.2:

     Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager
3. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.*x*:

     Click **Deployment Management**, and then click **Install Connector**.
   - For Oracle Identity Manager release 11.1.1:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.
   - For Oracle Identity Manager release 11.1.2:

     On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.
4. From the Connector List list, select **IBM RACF Standard 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 **IBM RACF Standard Connector *RELEASE_NUMBER*.**
5. Click **Load**.
6. To start the installation process, click **Continue**.

The following tasks are performed in sequence:

a. Configuration of connector libraries

b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager). If you want to import the target system as a trusted source for reconciliation, then see Section 2.3.1.4, "Configuring Trusted Source Reconciliation.".

c. Compilation of adapters

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

- Retry the installation by clicking **Retry.**
- Cancel the installation and begin again from Step 1.

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

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

---

Note: At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.

There are no prerequisites for some predefined connectors.

---

b. Configuring the IT resource for the connector

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

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

---

Note: In Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2.

See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

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

8. Copy files from the scripts directory on the connector installation media to the following location:

- For Oracle Identity Manager release 9.1.0.*x*: *OIM_HOME*/xellerate/RACFScripts
- For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/RACFScripts
- For Oracle Identity Manager release 11.1.2: *OIM_HOME*/server/RACFScripts

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

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorResources directory into the corresponding directories on each node of the cluster. See Section 2.1.1.1, "Files and Directories on the Installation Media" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.2.1.2 Configuring the IT Resource

Note: Perform this procedure if you are installing the connector on Oracle Identity Manager release 9.1.0.*x* or later.

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

1. Log in to the Administrative and User Console.
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.1.0.*x*:
     a. Expand **Resource Management,** and then click **Manage IT Resource.**
   - For Oracle Identity Manager release 11.1.1:
     a. On the Welcome page, click Advanced in the upper-right corner of the page.
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource.**
   - For Oracle Identity Manager release 11.1.2:
     a. On the Welcome page, click Advanced in the upper-right corner of the page.
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource.**
3. In the IT Resource Name field on the Manage IT Resource page, enter `RACF Server` and then click **Search**.
4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource. Table 2–2 describes each parameter.

Table 2–2 IT Resource Parameters

Parameter	Description
Admin	Administrator ID on the IBM RACF server
AdminCredential	Password of the admin ID account
Application	TSO value to which the admin user logs in. Sample value: `B`
Host	IP address or computer name of the mainframe system
Port	Port number at which the server is listening
LoginMacro	Name and directory path of the file that is used to reach the `READY` prompt on the IBM Mainframe server. The default value is as follows: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/ThirdParty/InitialLoginSequence.txt ■ For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/ThirdParty/InitialLoginSequence.txt ■ For Oracle Identity Manager release 11.1.2: *OIM_HOME*/server/ThirdParty/InitialLoginSequence.txt
AutoRetry	AutoRetry feature The value can be `YES` or `NO`. Default value: `NO`
AmountRetry	Number of retries for the AutoRetry feature Sample value: `2`
WaitTime	Wait time between consecutive retries Sample value: `20`
IsSecure	Specifies whether or not the connection between Oracle Identity Manager and IBM RACF must be secured by using SSL The value can be `YES` or `NO`. Default value: `NO` **Note:** It is recommended that you enable SSL to secure communication with the target system.
LogoutMacro	Name and directory path of the file that is used to exit from the `READY` prompt on the IBM Mainframe server. The default value is as follows: ■ For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*: *OIM_HOME*/xellerate/ThirdParty/LogOutSequence.txt ■ For Oracle Identity Manager release 11.1.1: *OIM_HOME*/server/ThirdParty/LogOutSequence.txt ■ For Oracle Identity Manager release 11.1.2: *OIM_HOME*/server/ThirdParty/InitialLoginSequence.txt

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

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

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

- Section 2.2.2.1, "Copying the Connector Files"
- Section 2.2.2.2, "Importing the Connector XML Files"
- Section 2.2.2.3, "Compiling Adapters"

2.2.2.1 Copying the Connector Files

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

> **See Also:** Section 2.1.1.1, "Files and Directories on the Installation Media" for more information about these files

File in the Installation Media Directory	Destination Directory
lib/xlUtilHostAccess.jar	*OIM_HOME*/xellerate/JavaTasks
lib/xlReconRACF.jar	*OIM_HOME*/xellerate/ScheduleTask
Files in the ext directory	*OIM_HOME*/xellerate/ThirdParty
Files in the scripts directory	*OIM_HOME*/xellerate/RACFScripts
Files in the resources directory	*OIM_HOME*/xellerate/connectorResources
Contents of the test directory	*OIM_HOME*/xellerate/XLIntegrations/racf
Files in the xml directory	*OIM_HOME*/XLIntegrations/racf/xml

> **Note:** In an Oracle Identity Manager cluster, copy the JAR files and the contents of the connectorResources directory to the corresponding directories on each node of the cluster.

2.2.2.2 Importing the Connector XML Files

To import the connector XML file into Oracle Identity Manager:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the RACFnonTrusted.xml file, which is in the *OIM_HOME*/XLIntegrations/racf/xml directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the RACF Server IT resource is displayed.
8. Specify values for the parameters of the RACF Server IT resource. See the table in Section 2.2.1.2, "Configuring the IT Resource" for information about the values to be specified.

9. Click **Next.** The Provide IT Resource Instance Data page for a new instance of the RACF Server IT resource type is displayed.
10. Click **Skip** to specify that you do not want to define another IT resource. The Confirmation page is displayed.

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

11. Click **View Selections**.

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

2.2.2.3 Compiling Adapters

Note: You must perform the procedure described in this section if you want to use the provisioning features of Oracle Identity Manager for this target system.

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

See Also: Section 1.6.6, "Provisioning Functions" for a listing of the provisioning functions that are available with this connector

- Create new RACF User
- RACF User Delete
- RACF User Enable
- addTsoToRacfUser
- setRacfUserPassword
- UpdateRacfUserAttribute
- connect to group
- Connect To Group
- removeTso
- RACF User Disable
- RACF Update Privilege
- PrepopulateRacfUsrId

You must compile these adapters before they can be used in provisioning operations.

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.

2. To compile all the adapters that you import into the current database, select **Compile All**.

   To compile multiple (but not all) adapters, select the adapters you want to compile. Then, select **Compile Selected**.

   Note: Click **Compile Previously Failed** to recompile only those adapters that were not compiled successfully. Such adapters do not have an `OK` compilation status.

3. Click **Start.** Oracle Identity Manager compiles the selected adapters.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the *OIM_HOME*/xellerate/Adapter directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes.

If you want to compile one adapter at a time, then use the Adapter Factory form.

See Also: *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms

To view detailed information about an adapter:

1. Highlight the adapter in the Adapter Manager form.
2. Double-click the row header of the adapter, or right-click the adapter.
3. Select **Launch Adapter** from the shortcut menu that is displayed. Details of the adapter are displayed.

2.3 Postinstallation

Postinstallation steps are divided across the following sections:

- Section 2.3.1, "Postinstallation on Oracle Identity Manager Server"
- Section 2.3.2, "Configuring SSL"
- Section 2.3.3, "Postinstallation on the Target System"

2.3.1 Postinstallation on Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

- Section 2.3.1.1, "Changing to the Required Input Locale"
- Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.3.1.3, "Enabling Logging"
- Section 2.3.1.4, "Configuring Trusted Source Reconciliation"
- Section 2.3.1.5, "Confuguring Request-Based Provisioning"

2.3.1.1 Changing to the Required Input Locale

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

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

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

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

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into the *OIM_HOME*/xellerate/connectorResources directory for Oracle Identity Manager release 9.1.0.*x*, and Oracle Identity Manager database for Oracle Identity Manager release 11.1.1 and release 11.1.2. Whenever you add a new resource bundle to the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, perform one of the following steps:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then switch to the *OIM_HOME*/xellerate/bin directory.
   - If you are using Oracle Identity Manager release 11.1.1, then switch to the *OIM_HOME*/server/bin directory.
   - If you are using Oracle Identity Manager release 11.1.2, then switch to the *OIM_HOME*/server/bin directory.

   Note: You must perform Step 1 before you perform Step 2. An exception is thrown if you run the command described in Step 2 as follows:

   For Oracle Identity Manager release 9.1.0.*x*:

   OIM_HOME/xellerate/bin/*SCRIPT_FILE_NAME*

   For Oracle Identity Manager release 11.1.1:

   OIM_HOME/server/bin/*SCRIPT_FILE_NAME*

   For Oracle Identity Manager release 11.1.2:

   OIM_HOME/server/bin/*SCRIPT_FILE_NAME*

2. Enter one of the following commands:

Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *`CATEGORY_NAME`* on Microsoft Windows or `PurgeCache.sh` *`CATEGORY_NAME`* on UNIX. The *`CATEGORY_NAME`* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

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

  On Microsoft Windows: `PurgeCache.bat ConnectorResourceBundle`

  On UNIX: `PurgeCache.sh ConnectorResourceBundle`

  Note: You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

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

  OIM_HOME/xellerate/config/xlconfig.xml

- For Oracle Identity Manager release 11.1.1:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

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

  `t3://`*`OIM_HOST_NAME`*`:`*`OIM_PORT_NUMBER`*

  In this format:

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

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

- For Oracle Identity Manager release 11.1.2:

  On Microsoft Windows: `PurgeCache.bat All`

  On UNIX: `PurgeCache.sh All`

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

  `t3://`*`OIM_HOST_NAME`*`:`*`OIM_PORT_NUMBER`*

  In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

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

2.3.1.3 Enabling Logging

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

- Section 2.3.1.3.1, "Enabling Logging on Oracle Identity Manager Release 9.1.0.x"
- Section 2.3.1.3.2, "Enabling Logging on Oracle Identity Manager Release 11.1.1"
-

2.3.1.3.1 Enabling Logging on Oracle Identity Manager Release 9.1.0.*x*

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

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL

  This level enables logging for all events.

- DEBUG

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

- INFO

  This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

  This level enables logging of information about error events that might allow the application to continue running.

- FATAL

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- OFF

  This level disables logging for all events.

The file in which you set the log level depends on the application server that you use:

- **IBM WebSphere Application Server**

To enable logging:

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

   ```
   log4j.logger.ADAPTER.RACFADAPTERLOGGER=log_level
   ```

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

   For example:

   ```
   log4j.logger.ADAPTER.RACFADAPTERLOGGER=INFO
   ```

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

WEBSPHERE_HOME/AppServer/logs/*SERVER_NAME*/SystemOut.log

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines if they are not already present in the file:

     ```
     <category name="ADAPTER.RACFADAPTERLOGGER">
        <priority value="log_level"/>
     </category>
     ```

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

     ```
     <category name="ADAPTER.RACFADAPTERLOGGER">
        <priority value="INFO"/>
     </category>
     ```

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

  JBOSS_HOME/server/default/log/server.log

- **Oracle Application Server**

  To enable logging:

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

     ```
     log4j.logger.ADAPTER.RACFADAPTERLOGGER=log_level
     ```

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

     For example:

     ```
     log4j.logger.ADAPTER.RACFADAPTERLOGGER=INFO
     ```

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

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

- **Oracle WebLogic Server**

  To enable logging:

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

     ```
     log4j.logger.ADAPTER.RACFADAPTERLOGGER=log_level
     ```

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

For example:

```
log4j.logger.ADAPTER.RACFADAPTERLOGGER=INFO
```

After you enable logging, log information is displayed on the server console.

2.3.1.3.2 Enabling Logging on Oracle Identity Manager Release 11.1.1

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

Oracle Identity Manager release 11.1.1 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

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

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

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

- CONFIG

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

- FINE, FINER, FINEST

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

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

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

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

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

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

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

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

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

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

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

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

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

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

<logger name="ADAPTER.RACFADAPTERLOGGER" level="NOTIFICATION:1"
useParentHandlers="false">
     <handler name="racf-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.

2.3.1.3.3 Enabling Logging on Oracle Identity Manager Release 11.1.2

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

Oracle Identity Manager release 11.1.2 uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.
- SEVERE

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

  This level enables logging of information about potentially harmful situations.
- INFO

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

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

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

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

Table 2–4 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1

Table 2–4 (Cont.) Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
WARNING	WARNING:1
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

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

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

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

To enable logging in Oracle WebLogic Server:

1. Edit the logging.xml file as follows:

   a. Add the following blocks in the file:

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

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

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

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

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

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

```
      <property name='maxLogSize' value='52428800'/>
      <property name='encoding' value='UTF-8'/>
    </log_handler>

<logger name="ADAPTER.RACFADAPTERLOGGER" level="NOTIFICATION:1"
useParentHandlers="false">
      <handler name="racf-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.

2.3.1.4 Configuring Trusted Source Reconciliation

While configuring the connector, the target system can be designated as a trusted source or target resource. If you designate the target system as a **trusted source**, then during a reconciliation run:

- For each newly created user on the target system, an OIM User is created.
- Updates made to each user on the target system are propagated to the corresponding OIM User.

If you designate the target system as a **target resource**, then during a reconciliation run:

- For each account created on the target system, a resource is assigned to the corresponding OIM User.
- Updates made to each account on the target system are propagated to the corresponding resource.

> **Note:** Skip this section if you do not want to designate the target system as a trusted source for reconciliation.

To configure trusted source reconciliation, you import the `RACFTrusted.xml` file while performing the procedure described in Section 2.2.2.2, "Importing the Connector XML Files."

Configuring trusted source reconciliation involves the following steps:

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

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

2. Set the value of the **isTrusted** scheduled task attribute to `Yes` while performing the procedure described in Section 3.3.4.1, "Submitjob User Reconciliation Scheduled Task."

To import the XML file for trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and 9.1.0.*x:*
     a. Click the **Deployment Management** link on the left navigation bar.
     b. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
   - For Oracle Identity Manager release 11.1.1:
     a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
   - For Oracle Identity Manager release 11.1.2:
     a. On the Welcome page, click **Advanced** in the upper-right corner of the page.
     b. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Import Deployment Manager File**. A dialog box for opening files is displayed.
3. Locate and open the **RACFTrusted.xml** file located in the following directory:
   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and release 9.1.0.*x*:

     OIM_HOME/xellerate/ConnectorDefaultDirectory/IBM_RACF_Std_90412/xml
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/ConnectorDefaultDirectory/IBM_RACF_Std_90412/xml
   - For Oracle Identity Manager release 11.1.2:

     OIM_HOME/server/ConnectorDefaultDirectory/IBM_RACF_Std_90412/xml

   Details of this XML file are shown on the File Preview page.
4. Click **Add File**. The Substitutions page is displayed.
5. Click **Next**. The Confirmation page is displayed.

6. Click **Import**.
7. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

2.3.1.5 Confuguring Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2 and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Administrative and User Console. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

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

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

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

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

- Section 2.3.1.5.1, "Copying Predefined Request Datasets"
- Section 2.3.1.5.2, "Importing Request Datasets into MDS"
- Section 2.3.1.5.3, "Enabling the Auto Save Form Feature"
- Section 2.3.1.5.4, "Running the PurgeCache Utility"

2.3.1.5.1 Copying Predefined Request Datasets

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

- ProvisionResource_RACF Server.xml
- ModifyProvisionedResource_RACF Server.xml

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

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\RACFStd

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

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

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

2.3.1.5.2 Importing Request Datasets into MDS

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

To import a request dataset definition into MDS:

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

   Note: While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.3.1.5.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\RACFStd directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

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

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

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

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

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

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

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

`t3://`*HOST_NAME_IP_ADDRESS*`:`*PORT*

In this format, replace:

- *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.
- *PORT* with the port on which Oracle Identity Manager is listening.

The request dataset is imported into MDS at the following location:

/custom/connector/*RESOURCE_NAME*

2.3.1.5.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **RACF User** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.3.1.5.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.3.1.2, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

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

2.3.2 Configuring SSL

Note: This is an optional step of the deployment procedure.

The CustomizedCAs.p12 file is the container for server certificates used for establishing an SSL connection. This file is compressed in the CustomizedCAs.jar file. The password for the CustomizedCAs.p12 file is `hod`. If the IBM Mainframe server has a certificate signed by a CA other than Verisign or Thawte, the root certificate of the CA must be added to the CustomizedCAs.p12 file for establishing the SSL connection.

The certificate can be added to the CustomizedCAs.p12 file by using a key management utility that supports PKCS12 format files. One of the tools that can be used to add the certificate is GSKkit7.0. This tool is part of IBM Host On-demand Server version 9.0.

To set up SSL connectivity between Oracle Identity Manager and the IBM Mainframe server:

1. Set the **IsSecure** parameter of the IT resource to `YES`.
2. Configure the target system to enable the required port for SSL connection.
3. If the certificate is issued by Thawte or any other well-known CA, then copy the WellKnownTrustedCertificatesCAs.jar file into the following directory:
   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and 9.1.0.*x:*

OIM_HOME/xellerate/lib/ThirdParty

- For Oracle Identity Manager release 11.1.1:

  OIM_HOME/server/lib/ThirdParty

- For Oracle Identity Manager release 11.1.2:

  OIM_HOME/server/lib/ThirdParty

4. Import the certificate in the CustomizedCAs.p12 file as follows:
   a. Extract the contents of the CustomizedCAs.jar file. This file is in the directory specified in Step 3.
   b. Add the SSL certificate in the CustomizedCAs.p12 file.
   c. Create the CustomizedCAs.jar file with the updated CustomizedCAs.p12 and CustomizedCAs.class files.
   d. Copy the updated JAR file into the directory specified in Step 3, depending on the Oracle Identity Manager release that you are using.

2.3.3 Postinstallation on the Target System

Postinstallation on the target system consists of the following steps:

1. Note down the Telnet and SSL port numbers specified in the TCP/IP profile file. When you configure the IT resource, you must provide these port numbers as part of the IT resource definition.
2. Using FTP, upload the members (scripts) from the *OIM_HOME*/xellerate/RACFScripts directory to a partitioned dataset with record length 80 and record format `Fixed Block`.
3. Upload the following file as a flat file or Physical Sequential (PS) file with record length 80 and record format `Fixed Block`.

   OIM_HOME/xellerate/RACFScripts/SYSTMDAT

   You must provide the following information in the `SYSTMDAT` file:

   - Name of the IBM RACF database dataset
   - Job header, which forms a part of the background job

     You must ensure that the job header contains the `NOTIFY` parameter in the following format:

     ```
     NOTIFY=&SYSUID
     ```

   - Name of the RACF source dataset containing the RACF scripts that you upload to a partitioned dataset on the IBM RACF server (in Step 2 of this procedure).
   - Region size and dynamic resource allocation values
   - Names of 10 temporary PS files that can be created and deleted by the connector

3

Using the Connector

This chapter contains the following sections:

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

3.1 Performing First-Time Reconciliation

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

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

> **Note:** In Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2, a scheduled job is an instance of a scheduled task. In this guide, the term **scheduled task** used in the context of Oracle Identity Manager release 9.1.0.*x* is the same as the term **scheduled job** in the context of Oracle Identity Manager release 11.1.1 and Oracle Identity Manager release 11.1.2.
>
> See *Oracle Fusion Middleware System Administrator's Guide for Oracle Identity Manager* for more information about scheduled tasks and scheduled jobs.

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

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

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

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

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

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

3.2 Lookup Field Synchronization

The RACF lookup fields reconciliation scheduled task is used for lookup fields reconciliation.

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

Note:

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

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

Attribute	Description
Server	Name of the IT resource instance that the connector uses to reconcile data Default value: `RACF Server`
LookupField Name	Name of the lookup field to be reconciled The value can be any one of the following: ▪ Lookup.RACF.Groups ▪ Lookup.RACF.Procedures ▪ Lookup.RACF.Accounts Default value: `Lookup.RACF.Groups`

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

Attribute	Description
LookupField Target File	Name of the file that you create on the target system server to store temporary data **Note:** You must create this file on the target system before you begin using the connector. Valid file name up to 8 characters in length Default value: `ADTTAR.NEW`
RACF Source Directory	Name of the directory on the IBM Mainframe server to which you copy the RACF scripts while performing the procedure described in Section 2.3.3, "Postinstallation on the Target System." Default value: `ADTTAR.DT250207.CNTL`
LookupType	Specifies the type of lookup reconciliation to be performed The value can be any one of the following: ■ Groups ■ Procedures ■ Accounts Default value: `Groups`

3.3 Configuring Reconciliation

Reconciliation involves duplicating in Oracle Identity Manager the creation of and modifications to user accounts on the target system. This section discusses the following topics related to configuring reconciliation:

- Section 3.3.1, "Full Reconciliation"
- Section 3.3.2, "Limited Reconciliation"
- Section 3.3.3, "Batched Reconciliation"
- Section 3.3.4, "Reconciliation Scheduled Tasks"

3.3.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

To perform a full reconciliation run:

- Ensure that the following schedules task attributes do not contain a value:
  - Filter Auditor Privilege (Y/N)
  - Filter Default Group
  - Filter Group Access Privilege (Y/N)
  - Filter Name
  - Filter Operations Privilege (Y/N)
  - Filter Owner
  - Filter Special Privilege (Y/N)
  - Filter User Id

  - Filter Type (AND/OR)

- Set the value of the Trial attribute of the user reconciliation scheduled task to `No`.

At the end of the reconciliation run, the Last Recon TimeStamp parameter of the GroupWise IT Resource IT resource is automatically set to the time stamp at which the run started. From the next reconciliation run onward, only records created or modified after this time stamp are considered for reconciliation. This is incremental reconciliation.

3.3.2 Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can customize this process by specifying the subset of added or modified target system records that must be reconciled. You do this by creating filters for the reconciliation module.

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

- Filter Auditor Privilege (Y/N)
- Filter Default Group
- Filter Group Access Privilege (Y/N)
- Filter Name
- Filter Operations Privilege (Y/N)
- Filter Owner
- Filter Special Privilege (Y/N)
- Filter User Id
- Filter Type (AND/OR)

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

The value of the Filter Type (AND/OR) attribute is applied to the rest of the filter attribute values that you specify. For example, suppose you specify the following values:

- Filter Default Group: `sales`
- Filter User Id: `jdoe`
- Filter Type (AND/OR): `AND`

When this scheduled task is run, records for which the user ID is jdoe and the default group value is sales are reconciled. If you were to specify OR as the value of the Filter Type (AND/OR) attribute, then records that satisfy any one filter criteria are reconciled.

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

3.3.3 Batched Reconciliation

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

You can configure batched reconciliation to avoid these problems.

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

- **Trial:** Use this attribute to specify whether to perform batched reconciliation. The default value is `Yes`.
- **trialCount:** Use this attribute to specify the total number of batches that must be reconciled. The default value is `All`.

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

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

- **Trial:** `Yes`
- **trialCount:** 10

Suppose that 314 user records were created or modified after the last reconciliation run. Of these 314 records, only 310 records would be reconciled during the current reconciliation run. The remaining 4 records would be reconciled during the next reconciliation run.

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

3.3.4 Reconciliation Scheduled Tasks

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

- Section 3.3.4.1, "Submitjob User Reconciliation Scheduled Task"
- Section 3.3.4.2, "GetData User Reconciliation Scheduled Task"

3.3.4.1 Submitjob User Reconciliation Scheduled Task

Fetching user data from the target system during reconciliation is a two-stage process. In the first stage, user data is extracted from the target system repository and copied to a file that you specify. In the second stage, the contents of the file are brought into Oracle Identity Manager.

The following scheduled tasks are used to submit the job that extracts user data and copies it into a file:

> **Note:** You must specify values for the attributes of one of these scheduled tasks.

- RACF submit job reconciliation
- RACF submit job trusted reconciliation

Table 3–2 describes the attributes of these scheduled tasks.

Note:

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

Table 3–2 Attributes of the Submitjob User Reconciliation Scheduled Tasks

Attribute	Description
Filter Type (AND/OR)	Specifies whether or not, and in what combination the specified filter conditions are to be used The value can be any one of the following: ■ AND to specify that you want reconciliation to be performed only if all the specified filter conditions are met. ■ OR to specify that you want reconciliation to be performed if any one or a combination of the specified filter conditions are met. ■ NODATA to specify that you do not want the filter conditions to be used. This is the default value. Default value: AND
RACF Database Name	Fully qualified name for the partitioned data set (PDS) containing the IBM RACF database Default value: ADTTAR.RACFBACK
System Parameter file Name	Fully qualified PS name used to upload the SYSTMDAT file Default value: ADTTAR.SYSTMDAT
Filter User Id	Specifies the user ID of the user account to be reconciled The value can be any one of the following: ■ User ID of the user account to be reconciled ■ NODATA to specify that this filter is to be ignored. This is the default value.
Filter Owner	Specifies the owner of the user accounts to be reconciled The value can be any one of the following: ■ User ID or group ID of the owner ■ NODATA to specify that this filter is to be ignored. This is the default value.
Filter Name	Specifies the Name value of the user accounts to be reconciled The value can be any one of the following: ■ Name value of the user accounts to be reconciled ■ NODATA to specify that this filter is to be ignored. This is the default value.
Filter Default Group	Specifies the default group of the user accounts to be reconciled The value can be any one of the following: ■ Default group ID of the user accounts to be reconciled ■ NODATA to specify that this filter is to be ignored. This is the default value.

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

Attribute	Description
Filter Operations Privilege (Y/N)	Specifies that user accounts with operations privileges are to be reconciled The value can be any one of the following: ■ Yes to specify that users with the Operations privilege are to be reconciled ■ No to specify that users with the Operations privilege are not to be reconciled ■ NODATA to specify that this filter is to be ignored. This is the default value. Default value: Yes
Filter Special Privilege (Y/N)	Specifies that user accounts with special privileges are to be reconciled The value can be any one of the following: ■ Yes to specify that users with the Special privilege are to be reconciled ■ No to specify that users with the Special privilege are not to be reconciled ■ NODATA to specify that this filter is to be ignored. This is the default value. Default value: Yes
Filter Group Access Privilege (Y/N)	Specifies that user accounts with the Group Access privilege are to be reconciled The value can be any one of the following: ■ Yes to specify that users with the Group Access privileges are to be reconciled ■ No to specify that users with the Group Access privileges are not to be reconciled ■ NODATA to specify that this filter is to be ignored. This is the default value. Default value: No
Filter Auditor Privilege (Y/N)	Specifies that user accounts with the Auditor privilege are to be reconciled The value can be any one of the following: ■ Yes to specify that users with the Auditor privilege are to be reconciled ■ No to specify that users with the Auditor privilege are not to be reconciled ■ NODATA to specify that this filter is to be ignored. This is the default value. Default value: No
Trial	Specifies whether or not batched reconciliation is to be carried out The value can be Yes or No. Default value: Yes
trialCount	Specifies the number of batches into which the reconciliation data is to be divided for the batched reconciliation run The value can be any natural number (1, 2, 3 . . .). Default value: 1
Target System Recon - Resource Object name	Name of the resource object Default value: RACF Server
Server	Name of the IT resource instance that the connector uses to reconcile data Default value: RACF Server
RACF Source Directory	Specifies the IBM RACF directory in which IBM RACF scripts are stored Default value: ADTTAR.DT281107.CNTL

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

Attribute	Description
Target System New User File	Name of the file that IBM RACF uses to store the latest image of the IBM RACF database Default value: `ADTTAR.NEW`
Target System Old User File	Name of the file that IBM RACF uses to store the old image of the IBM RACF database For first-time reconciliation, provide a dummy file name. You must ensure that this file does not exist on the IBM Mainframe. From the second reconciliation run onward, the value must be the same as the value of the Target System old User File attribute used during the first reconciliation run. Default value: `ADTTAR.OLDFILE.FRI112`
IsDebug	Specifies whether or not debugging must be performed The value can be `Yes` or `No`. Default value: `No`
isTrusted	A value of `Yes` implies that you want to configure the connector for trusted source reconciliation. A value of `No` implies that you want to configure the connector for target resource reconciliation. The default value of this attribute in the RACF submit job reconciliation scheduled task is `No`. The default value of this attribute in the RACF submit job trusted reconciliation scheduled task is `Yes`. **Note:** It is recommended that you do not change the value of this attribute.
File Path	Name and path of the file that stores information about the task running on the mainframe The next task checks this file to determine the status of the current task. Default value: `C:\RACF\Get.txt`

3.3.4.2 GetData User Reconciliation Scheduled Task

The following scheduled tasks are used to fetch user data from the file on the target system server to Oracle Identity Manager:

Note: You must specify values for the attributes of one of these scheduled tasks. You must configure the GetData scheduled task to run after the SubmitJob scheduled task.

- RACF getdata job reconciliation
- RACF getdata job trusted reconciliation

Table 3–3 describes the attributes of these scheduled tasks.

Note:

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

Table 3–3 Attributes of the GetData User Reconciliation Scheduled Tasks

Attribute	Description
Server	Name of the IT resource instance that the connector uses to reconcile data Default value: `RACF Server`
RACF Source Directory	Specifies the IBM RACF directory in which IBM RACF scripts are stored Default value: `ADTPKM.DT280507.REXX`
Target System Old User File	Name of the file that IBM RACF uses to store the old image of the IBM RACF database For first-time reconciliation, provide a dummy file name. You must ensure that this file does not exist on the IBM Mainframe. From the second reconciliation run onward, the value must be the same as the value of the Target System old User File attribute used during the first reconciliation run. Default value: `ADTTAR.OLDFILE.FRI112`
Job Name Path	Name and path of the file that stores information about the task running on the mainframe The next task checks this file to determine the status of the current task. Sample value: `C:/dummyfile.txt`
Target System Filter File	Specifies the fully qualified name of the PS file that is used to store filter file information Default value: `ADTTAR.RACF08.WORK`
System Parameter file Name	Specifies the fully qualified name of the PS file that is used to upload the `SYSTMDAT` file Default value: `ADTTAR.SYSTMDAT`
Target System Recon - Resource Object name	Name of the resource object Default value: `RACF Server`
isTrusted	A value of `Yes` implies that you want to configure the connector for trusted source reconciliation. A value of `No` implies that you want to configure the connector for target resource reconciliation. The default value of this attribute in the RACF getdata job reconciliation scheduled task is `No`. The default value of this attribute in the RACF getdata job trusted reconciliation scheduled task is `Yes`. **Note:** It is recommended that you do not change the value of this attribute.

3.4 Configuring Scheduled Tasks

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

Table 3–4 lists the scheduled tasks that form part of the connector.

Table 3–4 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
RACF lookup fields reconciliation	This lookup definition is used to synchronize the values of the lookup fields between Oracle Identity Manager and the target system. See Section 3.2, "Lookup Field Synchronization" for information about this scheduled task.
RACF submit job reconciliation	You use this scheduled task when the target system is configured as a target resource. This scheduled task is used to submit the job that extracts user data from the target system repository and copies to a file that you specify. In the second stage, the contents of the file are brought into Oracle Identity Manager. See Section 3.3.4.1, "Submitjob User Reconciliation Scheduled Task" for information about this scheduled task.
RACF submit job trusted reconciliation	You use this scheduled task when the target system is configured as a trusted source. This scheduled task is used to submit the job that extracts user data from the target system repository and copies to a file that you specify. In the second stage, the contents of the file are brought into Oracle Identity Manager. See Section 3.3.4.1, "Submitjob User Reconciliation Scheduled Task" for information about this scheduled task.
RACF getdata job reconciliation	You use this scheduled task when the target system is configured as a target resource. This scheduled task is used to fetch user data from the file on the target system server to Oracle Identity Manager. In the second stage, the contents of the file are brought into Oracle Identity Manager. See Section 3.3.4.2, "GetData User Reconciliation Scheduled Task" for information about this scheduled task.
RACF getdata job trusted reconciliation	You use this scheduled task when the target system is configured as a trusted source. This scheduled task is used to fetch user data from the file on the target system server to Oracle Identity Manager. In the second stage, the contents of the file are brought into Oracle Identity Manager. See Section 3.3.4.2, "GetData User Reconciliation Scheduled Task" for information about this scheduled task.

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

- Section 3.4.1, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.0.1 through 9.0.3.x"
- Section 3.4.2, "Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.x, Release 11.1.1, or Release 11.1.2"

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

To configure a scheduled task:

1. Open the Oracle Identity Manager Design Console.
2. Expand the **Xellerate Administration** folder.
3. Select **Task Scheduler.**
4. Click **Find**. The details of the predefined scheduled tasks are displayed on two different tabs.
5. For the first scheduled task, enter a number in the **Max Retries** field. Oracle Identity Manager must attempt to complete the task before assigning the `FAILED` status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.

7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task.

   See Also: *Oracle Identity Manager Design Console Guide* for information about adding and removing task attributes
10. Click **Save**. The scheduled task is created. The `INACTIVE` status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.

Stopping Reconciliation

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

1. Perform Steps 1 through 3 of the procedure to configure reconciliation scheduled tasks.
2. Select the **Stop Execution** check box in the task scheduler.
3. Click **Save**.

3.4.2 Configuring Scheduled Tasks on Oracle Identity Manager Release 9.1.0.*x*, Release 11.1.1, or Release 11.1.2

To configure a scheduled task:

1. Log in to the Administrative and User Console.
2. Perform one of the following:
   a. If you are using Oracle Identity Manager release 9.1.0.*x*, expand **Resource Management,** and then click **Manage Scheduled Task.**
   b. If you are using Oracle Identity Manager release 11.1.1, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
   c. If you are using Oracle Identity Manager release 11.1.2, then on the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. On the Scheduled Task Management page, enter the name of the scheduled task as the search criteria and then click **Search**.
     b. In the search results table, click the edit icon in the Edit column for the scheduled task.

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

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

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

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

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

- If you are using Oracle Identity Manager release 11.1.2, then:

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

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

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

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

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

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

      – **Max Retries:** Enter an integer value in this field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task. The default value is 1.

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

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

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

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

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

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

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

c. If you are using Oracle Identity Manager release 11.1.2, then on the Job Details tab, you can modify the following parameters:

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

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

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

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

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

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Attributes of the scheduled task are discussed in the following sections:

  Section 3.2, "Lookup Field Synchronization"

  Section 3.3.4, "Reconciliation Scheduled Tasks"

- If you are using Oracle Identity Manager release 9.1.0.*x*, then on the Attributes page, select the attribute from the Attribute list, specify a value in the field provided, and then click **Update**.
- If you are using Oracle Identity Manager release 11.1.1, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.
- If you are using Oracle Identity Manager release 11.1.2, then on the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

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

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

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

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

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

- If you are using Oracle Identity Manager release 11.1.2, then click **Apply** to save the changes.

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

3.5 Performing Provisioning Operations

Provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager.

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

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 3.6, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1 and Oracle Identity Manager Release 11.1.2."

This following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

See Also: *Oracle Identity Manager Connector Concepts* for information about the types of provisioning

This section discusses the following topics:

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

3.5.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Administrative and User Console.
2. If you want to first create an OIM User and then provision a target system account, then:
   - If you are using Oracle Identity Manager release 9.1.0.*x*, then:
     a. From the Users menu, select **Create**.

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

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

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

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

- If you are using Oracle Identity Manager release 11.1.2, then:

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

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

3. If you want to provision a target system account to an existing OIM User, then:

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

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

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

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

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

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

   - If you are using Oracle Identity Manager release 11.1.2, then:

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

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

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

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

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

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

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

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

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

   - If you are using Oracle Identity Manager release 11.1.2, then:

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

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

5. On the Step 1: Select a Resource page, select **RACF Server** from the list and then click **Continue**.
6. On the Step 2: Verify Resource Selection page, click **Continue**.
7. On the Step 5: Provide Process Data for Connect a RACF user to group page, if required, enter the relevant details and then click **Continue**.
8. On the Step 5: Provide Process Data for Add TSO parameters to user page, if required, enter the relevant details and then click **Continue**.
9. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue**.
10. The "Provisioning has been initiated" message is displayed. Perform one of the following steps:
    - If you are using Oracle Identity Manager release 9.1.0.*x*, click **Back to User Resource Profile.** The Resource Profile page shows that the resource has been provisioned to the user.
    - If you are using Oracle Identity Manager release 11.1.1, then:
      a. Close the window displaying the "Provisioning has been initiated" message.
      b. On the Resources tab, click **Refresh** to view the newly provisioned resource.
    - If you are using Oracle Identity Manager release 11.1.2, then:
      a. Close the window displaying the "Provisioning has been initiated" message.
      b. On the Resources tab, click **Refresh** to view the newly provisioned resource.

3.5.2 Request-Based Provisioning

Note: The information provided in this section is applicable only if you are using Oracle Identity Manager release 11.1.1 or Oracle Identity Manager release 11.1.2.

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

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

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

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

3.5.2.1 End User's Role in Request-Based Provisioning

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

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

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request**.

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next**.
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search**. A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next**.
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **RACF Server**, move it to the Selected Resources list, and then click **Next**.
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next**.
12. On the Justification page, you can specify values for the following fields, and then click **Finish**.
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the request ID, then the Request Details page is displayed.
14. To view details of the approval, on the Request Details page, click the **Request History** tab.

3.5.2.2 Approver's Role in Request-Based Provisioning

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

The following are steps that the approver can perform:

1. Log in to the Administrative and User Console.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task**.

   A message confirming that the task was approved is displayed.

3.6 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager Release 11.1.1 and Oracle Identity Manager Release 11.1.2

Note: It is assumed that you have performed the procedure described in Section 2.3.1.5, "Confuguring Request-Based Provisioning."

On Oracle Identity Manager release 11.1.1 or 11.1.2, 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 **RACF User** 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 **RACF Server** resource object.
   c. Deselect the Self Request Allowed check box.
   d. Click the Save icon.

On Oracle Identity Manager release 11.1.1 or 11.1.2, if you want to switch from direct provisioning 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 **RACF User** 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 **RACF Server** resource object.

c. Select the Self Request Allowed check box.

d. Click the Save icon.

4

Extending the Functionality of the Connector

After you deploy the connector, you might need to configure it to meet your business requirements. The following section describes the procedure that you can perform to extend the functionality of the connector.

4.1 Configuring the Connector for Multiple Installations of the Target System

> **Note:** Perform this procedure only if you want to configure the connector for multiple installations of IBM RACF.

You may want to configure the connector for multiple installations of IBM RACF. The following example illustrates this requirement:

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

To meet the requirement posed by such a scenario, you must configure the connector for multiple installations of IBM RACF.

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

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure

1. Create and configure one IT resource for each target system installation.

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

2. Configure reconciliation for each target system installation. See Section 3.4, "Configuring Scheduled Tasks" for instructions. Note that you only need to modify the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.

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

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

5

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. This chapter discusses the following topics related to connector testing:

5.1 Testing the Connector

You can use the testing utility to test basic connector functionality.

To use the testing utility:

1. Specify values for the parameters in the config.properties file. This file is located in the following directory:
   - For Oracle Identity Manager release 9.0.1 through 9.0.3.*x* and 9.1.0.*x:*

     OIM_HOME/xellerate/RACF/config
   - For Oracle Identity Manager release 11.1.1:

     OIM_HOME/server/RACF/config
   - For Oracle Identity Manager release 11.1.2:

     OIM_HOME/server/RACF/config

   These parameters are the same as the parameters of the IT resource.
2. Use the testing utility to perform the following tests:

   Note: The testing utility files are in the *OIM_HOME*/XLIntegrations/RACF directory.

   - Create an IBM RACF user.

     In the config.properties file, set the action to `CREATE_USER` and provide the user ID value for the `USER_ID` parameter.

     Save the changes and then run one of the following scripts:

     * For Microsoft Windows

       RACF.bat

     * For UNIX:

       RACF.sh

- Update an IBM RACF user.

  In config.properties file, set the action `UPDATE_USER` and provide the user ID and user attributes. The `attribute_name` parameter can be set to one of the following:

  * `NAME`: To update the name
  * `PASSWORD`: To update the password

  The `attribute_value` parameter is the value of the `attribute_name` to be changed. For example, if you set `attribute_name` to `NAME`, then `attribute_value` can be set to `John`.

  Save the changes and run the script.

- Delete an IBM RACF user.

  In the config.properties file, set the action to `DELETE_USER` and provide the user ID value for the `USER_ID` parameter.

  Save the changes and run the script.

5.2 Troubleshooting

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

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with the IBM Mainframe server	■ Ensure that the IBM Mainframe server is up and running. ■ Check if the user is already logged in. ■ Check if the user has been disabled on the IBM Mainframe server. ■ Check if Oracle Identity Manager is running. ■ Ensure that all the adapters have been compiled. ■ Use the IT Resources form to examine the Oracle Identity Manager record. Ensure that the IP address, admin ID, and admin password are correct. ■ Check the security parameters if an SSL connection is in use.
The Operation Failed message is displayed on the Oracle Identity Manager Administrative and User Console.	■ Ensure that the values for the attributes do not contain delimiter characters (such as white space, commas, apostrophes, and quotation marks). ■ Ensure that the attribute values do not exceed their permitted lengths.
Reconciliation fails	Ensure that the files specified for storing new user data on IBM RACF do not already exist on the server.
Provisioning operation fails while creating RACF Standard account if the user ID contains a special character such as _ (underscore) (for example, usr1_1)	Ensure that the user ID for RCAF Standard account follows the following rules in the RACF target system: ■ First character is A-Z, @, or #. ■ Other characters in the word can contain number from 0 to 9. ■ User ID must contain maximum 7 characters.
TSO ADD task shows rejected status in the target system even after the task is added to the target system.	This is the default behavior due to security reasons.

6

Known Issues

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

Index

R

S

T

U

V

X