Oracle® Identity Manager

Connector Guide for IBM RACF Standard

Release 9.0.4

E10156-01

May 2007

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

E10156-01

Primary Author: Shiladitya Guha

Contributing Authors: Deepa Aswani, Debapriya Datta, Lyju Vadassery

Contents

Preface

Oracle Identity Manager Connector Guide for IBM RACF Standard provides information about integrating Oracle Identity Manager with IBM RACF.

> **Note:** Some parts of the product and documentation still refer to the original Thor company name and Xellerate product name and will be rebranded in future releases.

Audience

This guide is intended for users who want to deploy the Oracle Identity Manager connector for IBM RACF Standard.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible, with good usability, to the disabled community. To that end, our documentation includes features that make information available to users of assistive technology. This documentation is available in HTML format, and contains markup to facilitate access by the disabled community. Accessibility standards will continue to evolve over time, and Oracle is actively engaged with other market-leading technology vendors to address technical obstacles so that our documentation can be accessible to all of our customers. For more information, visit the Oracle Accessibility Program Web site at

`http://www.oracle.com/accessibility/`

Accessibility of Code Examples in Documentation

Screen readers may not always correctly read the code examples in this document. The conventions for writing code require that closing braces should appear on an otherwise empty line; however, some screen readers may not always read a line of text that consists solely of a bracket or brace.

Accessibility of Links to External Web Sites in Documentation

This documentation may contain links to Web sites of other companies or organizations that Oracle does not own or control. Oracle neither evaluates nor makes any representations regarding the accessibility of these Web sites.

TTY Access to Oracle Support Services

Oracle provides dedicated Text Telephone (TTY) access to Oracle Support Services within the United States of America 24 hours a day, seven days a week. For TTY support, call 800.446.2398.

Related Documents

For more information, refer to the following documents in the Oracle Identity Manager documentation library:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation Guide for JBoss*
- *Oracle Identity Manager Installation Guide for Oracle Containers for J2EE*
- *Oracle Identity Manager Installation Guide for WebLogic*
- *Oracle Identity Manager Installation Guide for WebSphere*
- *Oracle Identity Manager Administrative and User Console Guide*
- *Oracle Identity Manager Administrative and User Console Customization Guide*
- *Oracle Identity Manager Design Console Guide*
- *Oracle Identity Manager Tools Reference Guide*
- *Oracle Identity Manager Audit Report Developer Guide*
- *Oracle Identity Manager Best Practices Guide*
- *Oracle Identity Manager Globalization Guide*
- *Oracle Identity Manager Glossary of Terms*

The following document is available in the Oracle Identity Manager Connector Pack documentation library:

- *Oracle Identity Manager Connector Framework Guide*

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack Release 9.0.4 documentation library, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in the Oracle Identity Manager Connector for IBM RACF?

This chapter provides an overview of the updates made to the software and documentation for the IBM RACF Standard connector in releases 9.0.3 of the Oracle Identity Manager connector pack.

> **See Also:** The 9.0.2 release of this guide for information about updates that were new for the 9.0.2 release

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

- Software Updates

  These include updates made to the connector software.

- Documentation-Specific Updates

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

> **See Also:** *Oracle Identity Manager Release Notes*

Software Updates

This section discusses updates made to this release of the connector software.

Enabling Logging

By following the instructions in the "Enabling Logging" section on page 2-3, you can configure the generation of log information that is specific to the target system.

Modification in Reconciliation Functionality

The following changes have been made in reconciliation functionality:

- Two tasks are used to perform user reconciliation. The first task generates reconciliation data. The second task collects the generated reconciliation data and sends it to Oracle Identity Manager.
- You can customize the reconciliation process by specifying the subset of added or modified target system records that must be reconciled. This feature is discussed in the "Partial Reconciliation" on page 3-1.
- In this release of the connector, user reconciliation scheduled task is added with attributes such as `BatchSize` and `NumberOfBatches`. By specifying values for

these attributes, you can reconcile users in various batches. These attributes are discussed in the "Batched Reconciliation" section on page 3-2.

- This release of the connector also supports trusted source reconciliation. This feature is discussed in the "Configuring Trusted Source Reconciliation" section on page 3-3.

  There are two connector XML files in the connector installation media directory, one each for trusted and nontrusted source reconciliation. These files are described in the "Files and Directories That Comprise the Connector" section on page 1-5. The procedure to describe either of these XML files is described in the "Step 6: Importing the Connector XML Files" section on page 2-7.

New User Reconciliation Scheduled Tasks

The user reconciliation scheduled task has been divided into two tasks. You can specify filter conditions that the reconciliation engine must apply during reconciliation. The attributes for these new scheduled tasks are described in the following sections:

- Submitjob User Reconciliation Scheduled Task on page 3-5
- GetData User Reconciliation Scheduled Task on page 3-8

Testing Utility

The testing utility has been added in this release of the connector. Information about the files that constitute this utility and the procedure to use it has been discussed in the "Running Test Cases" section on page 4-1.

Documentation-Specific Updates

The following documentation-specific updates have been made in this release of the guide:

- Instructions in the "Files and Directories That Comprise the Connector" section on page 1-5 have been revised.
- Instructions to enable logging for this connector are given in the "Enabling Logging" section on page 2-3.
- Some of the content from the Chapter 2 in earlier releases of this guide has been moved to Chapter 3.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with third-party applications. The connector for IBM RACF is used to integrate Oracle Identity Manager with IBM RACF Standard.

> **Note:** Oracle Identity Manager connectors were referred to as *resource adapters* prior to the acquisition of Thor Technologies by Oracle.

This chapter contains the following sections:

- Reconciliation Module
- Provisioning Module
- Supported Functionality
- Multilanguage Support
- Files and Directories That Comprise the Connector
- Determining the Release Number of the Connector

Reconciliation Module

Reconciliation involves duplicating in Oracle Identity Manager additions of and modifications to user accounts on the target system. It is an automated process initiated by a scheduled task that you configure.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations

Based on the type of data reconciled from the target system, reconciliation can be divided into the following types:

- Lookup Fields Reconciliation
- User Reconciliation

Lookup Fields Reconciliation

Lookup fields reconciliation involves reconciling the following lookup fields of IBM RACF:

- Group
- TSO Procedure
- TSO Account Number

User Reconciliation

User reconciliation involves reconciling the following user attributes in IBM RACF Standard.

Name	Description	Data Type
User General Data		
userid	User ID on the RACF system	String
owner	Owner of the user	String
name	Display name of the user	String
default group	Default group associated with the user	String
operations	Operations privilege	Number
auditor	Auditor privilege	Number
special	Special privilege	Number
grp access	Group access privilege	Number
department	Department name	String
User Group Data		
Groups	Child table	Multivalued attribute
group name	Group name	String
revoke date	Revoke date associated with group	String
authorization	Authorization privilege	String
User TSO Data		
TSO	Child table	Multivalued attribute
account number	TSO account number	String
procedure	TSO procedure name	String

Reconciled Xellerate User Fields

The following target system fields are reconciled only if trusted source reconciliation is implemented:

- User ID
- First Name
- Last Name
- Organization
- User Type
- Employee Type

Provisioning Module

Provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. You use the Administrative and User Console to perform provisioning operations.

> **See Also:** The "Deployment Configurations of Oracle Identity Manager" section in *Oracle Identity Manager Connector Framework Guide* for conceptual information about provisioning

For this target system, the following fields are provisioned:

- User Id
- RACF Server
- Password
- Owner
- Name
- Installation Data
- Default Group
- DEpartment
- Operations
- Auditor
- Special
- Group Access
- Group
- Revoke Date
- Authorization
- Account Number
- Procedure
- Size
- Unit
- Maximum Size

Supported Functionality

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

Function	Type	Description
Create RACF New User	Provisioning	Creates a user account
Delete a RACF User	Provisioning	Deletes a user account
Name Updated	Provisioning	Changes the name of a user account
Password Updated	Provisioning	Changes the password of a user account
Owner Updated	Provisioning	Changes the owner of a user account

Function	Type	Description
Department Updated	Provisioning	Changes the department of a user account
Default Group Updated	Provisioning	Changes the default group of a user account
Installation data Updated	Provisioning	Changes the installation data of a user account Installation data is a field that can contain any installation, system, or project-related data.
Operations Updated	Provisioning	Changes the Operations attribute of a user account
Special Updated	Provisioning	Changes the Special attribute of a user account
Auditor Updated	Provisioning	Changes the Auditor attribute of a user account
Group Access Updated	Provisioning	Changes the Group Access attribute of a user account
Enables a RACF User	Provisioning	Enables a user account so that the user is able to log in to the IBM Mainframe server
Disables a RACF User	Provisioning	Disables a user account so that the user is not able to log in to the IBM Mainframe server
Connect Group	Provisioning	Connects a user to a group in IBM RACF
Disconnect Group	Provisioning	Removes a user from a group in IBM RACF
Add TSO to a User	Provisioning	Provides Time Sharing Options (TSO) access to a user TSO is one of the subsystems in z/OS in IBM Mainframes.
Remove TSO	Provisioning	Removes TSO access from a user
Reconcile Lookup Field	Reconciliation	Reconciles the lookup fields
Reconcile User Data	Reconciliation	Reconciles user data

See Also: Appendix A for information about attribute mappings between Oracle Identity Manager and IBM RACF Standard.

Multilanguage Support

The connector supports the following languages:

- Chinese Simplified
- Chinese Traditional
- English
- French
- German
- Italian
- Japanese

- Korean
- Portuguese (Brazilian)
- Spanish

Note: IBM RACF does not support the entry of non-ASCII characters. Refer to Chapter 5 for more information about this limitation.

See Also: *Oracle Identity Manager Globalization Guide* for information about supported special characters

Files and Directories That Comprise the Connector

The files and directories that comprise this connector are compressed in the following directory on the installation media:

```
Security Applications/IBM RACF/IBM RACF Standard
```

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`lib/JavaTask/xlUtilHostAccess.jar`	This JAR file contains the class files that are required for provisioning.
`lib/ScheduleTask/xlReconRACF.jar`	This JAR file contains the class files that are required for reconciliation.
`lib/ext/CustomizedCAs.jar`	This file is used to set up an SSL connection between Oracle Identity Manager and the IBM Mainframe server.
`lib/ext/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.
`lib/ext/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.
`lib/ext/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.

File in the Installation Media Directory	Description
Scripts/DATAEXTT	This file uses the decrypted copy of the IBM RACF database to extract user-related records required for reconciliation into temporary files. It is a member of a procedure library on the IBM Mainframe server.
Scripts/DATAUNLD	This file merges the data from the SYSTMDAT and JCLSRC files into 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 bundle files contains language-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.

File in the Installation Media Directory	Description
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. 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.

The "Step 5: Copying External Code Files" section on page 2-6 provides instructions to copy these files into the required directories.

Determining the Release Number of the Connector

You can use any one of the following methods to determine the release number of the connector.

Before Deployment

To determine the release number of a connector:

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

   ```
   Security Applications/IBM RACF/IBM RACF Standard/lib/ScheduleTask
   ```

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

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

Note: If you maintain a copy of the `xlReconRACF.jar` file after deployment, you can use this method to determine the release number of the connector at any stage. After you deploy the connector, it is recommended that you use the "After Deployment" method, which is described in the following section.

After Deployment

To determine the release number of a connector that has already been deployed:

See Also: *Oracle Identity Manager Design Console Guide*

1. Open the Oracle Identity Manager Design Console.
2. In the Form Designer, open the process form. The release number of the connector is the value of the **Version** field.

2

Deploying the Connector

Deploying the connector involves the following steps:

- Step 1: Verifying Deployment Requirements
- Step 2: Copying the Connector Files
- Step 3: Configuring the Oracle Identity Manager Server
- Step 4: Configuring the Target System
- Step 5: Copying External Code Files
- Step 6: Importing the Connector XML Files
- Step 7: Configuring SSL

Step 1: Verifying Deployment Requirements

The following table lists the deployment requirements for the connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3 or later
Target systems	IBM RACF on z/OS 1.4
Target system host platforms	z/OS 1.4
External code	The following Host Access Class Library (HACL) class files obtained from IBM Host On-Demand (HOD) version 9.0: ■ `hoddbg2.jar` ■ `hacp.jar` ■ `hasslite2.jar` ■ `habasen2.jar` ■ `WellKnownTrustedCAs.class` ■ `WellKnownTrustedCAs.p12`

Item	Requirement
Target system user account	Instructions to create an IBM RACF user account with the required privileges are given in the "Step 4: Configuring the Target System" section on page 2-5. You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-7. 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.

Step 2: Copying the Connector Files

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

Note: The directory paths given in the first column of this table correspond to the location of the connector files in the following ZIP file on the installation media:

```
Security Applications/IBM RACF/IBM RACF Standard
```

Refer to the "Files and Directories That Comprise the Connector" section on page 1-5 for more information about these files.

File in the Installation Media Directory	Destination Directory
lib/JavaTask/xlUtilHostAccess.jar	*OIM_home*/xellerate/JavaTasks
lib/ScheduleTask/xlReconRACF.jar	*OIM_home*/xellerate/ScheduleTask
Files in the lib/ext directory	*OIM_home*/xellerate/ext
Files in the Scripts directory	*OIM_home*/xellerate/Scripts
Files in the resources directory	*OIM_home*/xellerate/connectorResources
Files in the xml directory	*OIM_home*/xlclient/xml

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

Step 3: Configuring the Oracle Identity Manager Server

Configuring the Oracle Identity Manager server involves the following procedures:

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

- Changing to the Required Input Locale

- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

Changing to the Required Input Locale

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

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

Clearing Content Related to Connector Resource Bundles from the Server Cache

While performing the instructions described in the "Step 2: Copying the Connector Files" section on page 2-2, you copy files from the `resources` directory on the installation media into the *OIM_home*`/xellerate/connectorResources` directory. Whenever you add a new resource bundle in the `connectorResources` directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

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

1. In a command window, change to the *OIM_home*`/xellerate/bin` directory.

   Note: You must perform Step 1 before you perform Step 2. If you run the command described in Step 2 as follows, then an exception is thrown:

   ```
   OIM_home\xellerate\bin\batch_file_name
   ```

   ---

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   Note: You can ignore the exception that is thrown when you perform Step 2.

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

   ```
   OIM_home/xellerate/config/xlConfig.xml
   ```

Enabling Logging

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

- `ALL`

This level enables logging for all events.

- DEBUG

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

- INFO

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

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

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

- FATAL

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

- OFF

  This level disables logging for all events.

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

- **BEA WebLogic**

  To enable logging:

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

     ```
     log4j.logger.Adapter.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:

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

- **IBM WebSphere**

  To enable logging:

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

     ```
     log4j.logger.Adapter.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*/startServer.log

- **JBoss Application Server**

  To enable logging:

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

     ```
     <category name="Adapter.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

- **OC4J**

  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:

  OC4J_home/opmn/logs/default_group~home~default_group~1.log

Step 4: Configuring the Target System

To configure the target system:

1. Note down the Telnet and SSL port numbers specified in the TCP/IP profile file. When you perform the "Defining IT Resources" procedure, 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/Scripts 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/Scripts/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

4. Create a user on the IBM Mainframe server with TSO access using an existing user account to which the `Special` attribute has been assigned.
5. 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
   ```

6. 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
   ```

7. 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
   ```

Step 5: Copying 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>
   ```

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:

   ```
   OIM_home/Xellerate/ext
   ```

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

   OIM_home/Xellerate/ext

Step 6: 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 locating files is displayed.
4. Locate and open the `RACFnonTrusted.xml` file, which is in the *OIM_home*/xlclient directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File.** The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next.** The Provide IT Resource Instance Data page for the `RACF Server` IT resource is displayed.
8. Specify values for the parameters of the `RACF Server` IT resource. Refer to the "Defining IT Resources" section on page 2-7 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 Tools Reference Guide* for instructions.

11. Click **View Selections**.

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

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

After you import the connector XML file, proceed to the "Step 7: Configuring SSL" section on page 2-8.

Defining IT Resources

You must specify values for the `RACF Server` IT resource parameters listed in the following table.

Parameter	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. Value: *`OIM_home`*`/ext/loginsequence.txt`
`AutoRetry`	AutoRetry feature The value can be `YES` or `NO.` The default value is `NO.`
`AmountRetry`	Number of retries for the AutoRetry feature Sample value: `2` or `5`
`WaitTime`	Wait time between consecutive retries Sample value: `20` or `30`
`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.` The default value is `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. Value: *`OIM_home`*`/ext/logoutsequence.txt`
`IsDebug`	Specifies whether or not debugging must be performed The value can be `YES` or `NO`. The default value is `NO`.

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

Step 7: 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:

   ```
   OIM_home/xellerate/lib/ext
   ```

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 following directory:

      ```
      OIM_home/xellerate/lib/ext
      ```

   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 following directory:

      ```
      OIM_home/Xellerate/ext
      ```

3 Configuring the Connector

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

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

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

Configuring Reconciliation

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

- Partial Reconciliation
- Batched Reconciliation
- Configuring Trusted Source Reconciliation
- Configuring the Reconciliation Scheduled Tasks

Partial 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.

While deploying the connector, follow the instructions in the "Specifying Values for the Scheduled Task Attributes" section on page 3-4 to specify values for these attributes and the logical operator that you want to apply.

Batched Reconciliation

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

You can configure batched reconciliation to avoid these problems.

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

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

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

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

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

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

You specify values for the `BatchSize` and `NumberOfBatches` attributes by following the instructions described in the "Specifying Values for the Scheduled Task Attributes" section on page 3-4.

Configuring Trusted Source Reconciliation

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

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

To configure trusted source reconciliation, you import the `RACFTrusted.xml` file while performing the procedure described in the "Step 6: Importing the Connector XML Files" section on page 2-7.

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 the "Submitjob User Reconciliation Scheduled Task" section on page 3-5.

To configure trusted source reconciliation:

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation bar.
3. Click the **Import** link under Deployment Management. A dialog box for locating files is displayed.
4. Locate and open the `RACFTrusted.xml` file, which is in the *`OIM_home`*`/xlclient` directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the **XML** file and then click **OK**.

Configuring the Reconciliation Scheduled Tasks

When you perform the procedure described in the "Step 6: Importing the Connector XML Files" section on page 2-7, the scheduled tasks for lookup fields, trusted source user, and nontrusted user reconciliations are automatically created in Oracle Identity Manager. To configure these scheduled tasks:

1. Open the Oracle Identity Manager Design Console.
2. Expand the Xellerate Administration folder.
3. Select **Task Scheduler**.
4. Click **Find**. The details of the predefined scheduled tasks are displayed.
5. Enter a number in the Max Retries field. This number represents the number of times Oracle Identity Manager must attempt to complete the task before assigning the ERROR status to the task.
6. Ensure that the **Disabled** and **Stop Execution** check boxes are not selected.
7. In the Start region, double-click the **Start Time** field. From the date-time editor that is displayed, select the date and time at which you want the task to run.
8. In the Interval region, set the following schedule parameters:
   - To set the task to run on a recurring basis, select the **Daily**, **Weekly**, **Recurring Intervals**, **Monthly**, or **Yearly** option.

     If you select the **Recurring Intervals** option, then you must also specify the time interval at which you want the task to run on a recurring basis.
   - To set the task to run only once, select the **Once** option.
9. Provide values for the attributes of the scheduled task. Refer to the "Specifying Values for the Scheduled Task Attributes" section on page 3-4 for information about the values to be specified.
10. Click **Save**. The scheduled task is created. The INACTIVE status is displayed in the **Status** field, because the task is not currently running. The task is run at the date and time that you set in Step 7.
11. Repeat Steps 5 through 10 to create the second scheduled task.

After you create both scheduled tasks, proceed to the "Configuring Provisioning" section on page 3-9.

Specifying Values for the Scheduled Task Attributes

This section provides information about the values to be specified for the following scheduled tasks:

- Lookup Fields Reconciliation Scheduled Task
- Submitjob User Reconciliation Scheduled Task
- GetData User Reconciliation Scheduled Task

Lookup Fields Reconciliation Scheduled Task You must specify values for the following attributes of the `RACF lookup fields reconciliation` lookup fields reconciliation scheduled task.

Note:

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

Attribute	Description	Sample Value
`Server`	Name of the IT resource instance that the connector uses to reconcile data	`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`
`LookupField Target File`	Name of the file that the connector creates on the IBM Mainframe server to temporarily store data	Valid file name up to 8 characters in length For example: `temp` and `work1`
`RACF Source Directory`	Name of the directory on the IBM Mainframe server in which RACF scripts are stored	`ADTTAR.DT250207.CNTL`
`IsDebug`	Specifies whether or not debugging must be performed	The value can be `YES` or `NO`. The default value is `NO`.

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

Submitjob User Reconciliation Scheduled Task You must specify values for the following attributes of the Submitjob user reconciliation scheduled task:

- RACF submit job reconciliation
- RACF submit job trusted reconciliation

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.

Attribute	Description	Value
`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.
`RACF Database Name`	Fully qualified name for the partitioned data set (PDS) containing the IBM RACF database	Sample value: `SYS1.ACMEY.RACFBACK`
`System Parameter file Name`	Fully qualified PS name used to upload the `SYSTMDAT` file	Sample 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.
`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.

Attribute	Description	Value
`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.
`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 privilege are to be reconciled ■ `No` to specify that users with the Group Access privilege are not to be reconciled ■ `NODATA` to specify that this filter is to be ignored. This is the default value.
`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.
`Trial`	Specifies whether or not trial reconciliation is to be carried out	The value can be `Yes` or `No`.
`trialCount`	Specifies the number of batches into which the reconciliation data is to be divided for the trial run	The value can be any natural number (1, 2, 3 . . .).
`Target System Recon - Resource Object name`	Name of the resource object	Resource object name Sample value: `RACF Server`
`Server`	Name of the IT resource instance that the connector uses to reconcile data	IT Resource Instance name Sample value: `RACF Server`
`RACF Source Directory`	Specifies the IBM RACF directory in which IBM RACF scripts are stored	Sample value: `ADTTAR.DT250207.CNTL`
`Target System New User File`	Name of the file that IBM RACF uses to store the latest image of the IBM RACF database	Fully qualified PDS name Sample value: `adttar.new`

Attribute	Description	Value
`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.	Fully qualified PDS name Sample value: `adttar.oldfile.fri112`
`IsDebug`	Specifies whether or not debugging must be performed	The value can be `Yes` or `No`. The default value is `No`.
`IsTrusted`	Specifies whether or not trusted source reconciliation is to be performed	The value can be `Yes` or `No`.
`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.	Sample value: `C:/dummyfile.txt`

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

GetData User Reconciliation Scheduled Task You must specify values for the following GetData user reconciliation scheduled task:

- `RACF getdata job reconciliation`
- `RACF getdata job trusted reconciliation`

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.

Attribute	Description	Value
`Server`	Name of the IT resource instance that the connector uses to reconcile data	IT Resource Instance name For example, RACF Server
`RACF Source Directory`	Specifies the IBM RACF directory in which IBM RACF scripts are stored	`ADTTAR.DT250207.CNTL`

Attribute	Description	Value
`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.	Fully qualified PDS name Sample 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	Sample 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	Sample value: `adttar.systmdat`
`Target System Recon - Resource Object name`	Name of the resource object	Resource object name Sample value: `RACF Server`

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

Configuring Provisioning

As mentioned earlier in this guide, provisioning involves creating or modifying a user's account information on the target system through Oracle Identity Manager. Refer to the "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector.

Note: You must perform this procedure if you want to use the provisioning features of the connector.

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

See Also: The "Supported Functionality" section on page 1-3 for a listing of the provisioning functions that are available with this connector

- `adpCREATENEWRACFUSER`
- `adpRACFUSERDELETE`
- `adpRACFUSERENABLE`
- `adpADDTSOTORACFUSER`
- `adpSETRACFUSERPASSWORD`

- adpUPDATERACFUSERATTRIBUTE
- adpCONNECTTOGROUP
- adpDISCONNECTFROMGROUP
- adpREMOVETSO
- adpRACFUSERDISABLE
- adpRACFUPDATEPRIVILEDGE

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.

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 Acme 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. Refer to the "Configuring Reconciliation" section on page 3-1 for instructions. Note that you only need to modify the attributes that are used to specify the IT resource and to specify whether or not the target system installation is to be set up as a trusted source.

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

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.

4

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:

- Running Test Cases
- Troubleshooting

Running Test Cases

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

In a command window, change to the directory in which the `xlutilHostAccess.jar` file is present. This file is in the *`OIM_home`*`/Xellerate/JavaTasks` directory. This utility uses some files from the `ext` directory.

Then, use the testing utility to perform the following tests:

- Create an IBM RACF user by entering the following command:

  ```
   java -jar xlUtilHostAccess.jar 1 user_id
  ```

- Update an IBM RACF user by entering the following command:

  ```
  java -jar xlUtilHostAccess.jar 3 user_id attribute_name attribute_value
  ```

  In this command, *`attribute_name`* can be set to one of the following:

  - `NAME:` To update the name
  - `PASSWORD:` To update the password
  - `OWNER:` To update the owner
  - `DFLTGRP:` To update the default group
  - `DATA:` To update the installation data

- Delete an IBM RACF user by entering the following command:

  ```
  java -jar xlUtilHostAccess.jar 2 user_id
  ```

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.

5 Known Issues

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

- The connector does not support trusted source reconciliation.
- Only one TSO set can be provisioned to a particular user. If more than one TSO set is provisioned to a user, then only the TSO set provisioned last would be valid.
- The following functions are not supported:
  - Update User's Address
  - Assign Profile to a User
  - Remove Profile from a User
  - Add a Profile
  - Remove a Profile
  - Update a Profile
- IBM RACF does not support the entry of non-ASCII characters. Therefore, you cannot transfer non-ASCII data through the connector. However, error messages and response codes would be displayed in Oracle Identity Manager in the language that you select.

A

Attribute Mappings Between Oracle Identity Manager and IBM RACF

The following table discusses attribute mappings between Oracle Identity Manager and IBM RACF.

Oracle Identity Manager Attribute	IBM RACF Field	Description
userid	USBD_NAME	User ID as taken from the profile name
owner	USBD_OWNER_ID	User ID or group that owns the profile
name	USBD_PROGRAMMER	Name associated with the user ID
default group	USBD_DEFGRP_ID	Default group associated with the user
operations	USBD_OPER	Specifies whether or not the user has the OPERATIONS attribute (Yes/No)
auditor	USBD_AUDITOR	Specifies whether or not the user has the AUDITOR attribute (Yes/No)
special	USBD_SPECIAL	Specifies whether or not the user has the SPECIAL attribute (Yes/No)
grp access	USBD_GRPACC	Specifies whether or not the user has the GRPACC attribute (Yes/No)
department	USWRK_DEPARTMENT	Department for delivery
group name	USCON_GRP_ID	Group to which the user is associated
revoke date	USCON_REVOKE_DATE	Date that the user's association to the group will be revoked
authorization	GPMEM_AUTH	Indicates the authority that the user ID has within the group Valid values are USE, CONNECT, JOIN, and CREATE.
account number	USTSO_ACCOUNT	Default account number
procedure	USTSO_LOGON_PROC	Default logon procedure

Index