Oracle® Identity Manager

Connector Guide for IBM RACF Standard

Release 9.0.3

B32353-01

February 2007

ORACLE®

Oracle Identity Manager Connector Guide for IBM RACF Standard, Release 9.0.3

B32353-01

Contents

3 Testing and Troubleshooting

4 Known Issues

A Attribute Mappings Between Oracle Identity Manager and IBM RACF

Index

Preface

Oracle Identity Manager Connector Guide for IBM RACF 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.

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 9.0.2 connector documentation set, 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 connector and documentation for IBM RACF 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.

Enhancement in the Multilanguage Support Feature

In addition to the three languages supported by the earlier release, this release of the connector supports seven new languages. All the supported languages are listed in the "Multilanguage Support" section on page 1-2.

> **Note:** IBM RACF does not support the entry of non-ASCII characters. Refer to Chapter 4 for more information about this limitation.

Support for OC4J

Earlier releases of the connector supported the following application servers:

- JBoss Application Server
- BEA WebLogic
- IBM WebSphere

This release of the connector also supports Oracle Containers for J2EE (OC4J).

Documentation-Specific Updates

The following documentation-specific update has been made in this release of the guide:

- In the "Step 7: Compiling Adapters" section on page 2-12, the instruction about restarting the node has been removed from Step 4 of the procedure to compile adapters.

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.

> **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:

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

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
Department Updated	Provisioning	Changes the department of a user account
Default Group Updated	Provisioning	Changes the default group of a user account

Function	Type	Description
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.

Multilanguage Support

This release of the connector supports the following languages:

- English
- Brazilian Portuguese
- French
- German
- Italian
- Japanese
- Korean
- Simplified Chinese
- Spanish

- Traditional Chinese

Note: IBM RACF does not support the entry of non-ASCII characters. Refer to Chapter 4 for more information about this limitation.

Reconciliation Module

This section discusses the elements that the reconciliation module extracts from the target system to construct reconciliation event records.

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.

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		

Name	Description	Data Type
TSO	Child table	Multivalued attribute
account number	TSO account number	String
procedure	TSO procedure name	String

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\ThirdParty\CustomizedCAs.jar	This file is used to set up an SSL connection between Oracle Identity Manager and the IBM Mainframe server.
lib\ThirdPartyI\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\ThirdParty\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 troubleshooting utility.
lib\ThirdParty\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.
RACF 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.
RACF 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.

File in the Installation Media Directory	Description
RACF 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.
RACF 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.
RACF Scripts\RECNLKUP	This file provides lookup fields data. It is a member of a procedure library on the IBM Mainframe server.
RACF 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.
RACF 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.
RACF 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.
RACF 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.
RACF 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.
RACF 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.
RACF 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.
xml\racfResAdp.xml	This XML file contains definitions for the following components of the connector: ■ IT resource type ■ IT resource ■ Resource object form ■ Process definition ■ Process tasks ■ Connector tasks

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

Determining the Release Number of the Connector

To determine the release number of the connector that you have deployed:

1. Extract the contents of the `xlReconRACF.jar` file. For a connector that has been deployed, this file is in the following directory:

   OIM_home\xellerate\JavaTasks

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.

   > **See Also:** *Oracle Identity Manager Design Console Guide*

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
- Step 6: Importing the Connector XML Files
- Step 7: Configuring Reconciliation
- Step 8: Compiling Adapters
- Step 9: Configuring SSL

If you want to configure the connector for multiple installations of IBM RACF, then perform the following procedure:

- Configuring the Connector for Multiple Installations of the Target System

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 Mainframe Server
Target system host platforms	RACF on 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 2-3.
	You provide the credentials of this user account while performing the procedure in the "Defining IT Resources" section on page 2-6.

Step 2: Copying the Connector Files

Copying the connector files involves the following steps:

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 1-4 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\ThirdParty` directory	*OIM_home*\xellerate\ThirdParty
Files in the `RACF Scripts` directory	*OIM_home*\xellerate\RACF Scripts
Files in the `resources` directory	*OIM_home*\xellerate\connectorResou rces
`xml\racfResAdp.xml`	*OIM_home*\xlclient\

> **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](#)

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.

To set the required input locale:

> **Note:** Depending on the operating system used, you may need to perform this procedure differently.

1. Open Control Panel.

2. Double-click **Regional Options**.

3. On the Input Locales tab of the Regional Options dialog box, add the input locale that you want to use and then switch to the input locale.

Clearing Content Related to Connector Resource Bundles from the Server Cache

Whenever you add a new resource bundle in the *OIM_home*\xellerate\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.

2. Enter one of the following commands:

> **Note:** You must perform Step 1 before you perform this step. If you run the command as follows, then an exception is thrown:
>
> *OIM_home*\xellerate\bin*batch_file_name*

■ On Microsoft Windows:

```
PurgeCache.bat ConnectorResourceBundle
```

■ On UNIX:

```
PurgeCache.sh ConnectorResourceBundle
```

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

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

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\RACF 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\RACF 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

   The name of this file must start with the high-level qualifier of the user ID that is used to perform reconciliation. For example, it can be named as *XX*.SYSTMDAT, where *XX* is the user ID on the IBM Mainframe server that is used to run reconciliation.

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

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\ThirdParty`

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\ThirdParty`

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 `racfResAdp.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 2-6 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. Remove these nodes 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 Reconciliation" section on page 2-7.

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*\ThirdParty\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*\ThirdParty\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 Reconciliation

Configuring reconciliation involves creating the reconciliation 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 2-7 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 "Step 8: Compiling Adapters" section on page 2-9.

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
- User Reconciliation Scheduled Task

Lookup Fields Reconciliation Scheduled Task

You must specify values for the following attributes of the 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.

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.

User Reconciliation Scheduled Task

You must specify values for the following attributes of the user 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.

Attribute	Description	Value
Target System Recon - Resource Object name	Name of the resource object	Resource object name For example, RACF Server
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
Target System New User File	Name of the file that IBM RACF uses to store the latest image of the IBM RACF database	Valid file name up to 8 characters in length Sample value: Recon or Userrecn

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	Valid file name up to 8 characters in length
	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.	
`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.

Step 8: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

- `adpCREATENEWRACFUSER`

- `adpRACFUSERDELETE`

- `adpRACFUSERENABLE`

- `adpADDTSOTORACFUSER`

- `adpSETRACFUSERPASSWORD`

- `adpUPDATERACFUSERATTRIBUTE`

- `adpCONNECTTOGROUP`

- `adpDISCONNECTFROMGROUP`

- `adpREMOVETSO`

- `adpRACFUSERDISABLE`

- `adpRACFUPDATEPRIVILEDGE`

You must compile these adapters before you can use them to provision accounts on the target system.

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 the **Compile All** option.

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

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.

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.

> **Note:** To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about using the Adapter Factory and Adapter Manager forms.

Step 9: 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\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 following directory:

      OIM_home\xellerate\lib\ThirdParty

   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\ThirdParty

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. Refer to *Oracle Identity Manager Design Console Guide* for detailed instructions on performing each step of this procedure.

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

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

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

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

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

3. Design one process form for each resource object.

   The Form Designer form is in the Development Tools folder. The following process forms are created when you import the connector XML file:

   - `UD_DB_RACF` (main form)

   - `UD_CO_GROUP` and `UD_ADD_TSO` (child forms)

   You can use these process forms as templates for creating the remaining process forms.

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

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

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

   - From the **Object Name** lookup field, select the resource object that you create in Step 1.

   - From the **Table Name** lookup field, select the process form that you create in Step 3.

   - While mapping the adapter variables for the IT Resource data type, ensure that you select the IT resource that you create in Step 2 from the **Qualifier** list.

5. Configure reconciliation for each target system installation. Refer to the "Step 7: Configuring Reconciliation" section on page 2-7 for instructions. Note that only the values of the following attributes are to be changed for each reconciliation scheduled task:

   - `Target System Recon - Resource Object name`

   - `Server`

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

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

3

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 troubleshooting 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 `ThirdParty` directory.

Then, use the troubleshooting 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.

4

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