Oracle® Identity Manager

Connector Guide for IBM RACF

Release 9.0.1

B31116-01

June 2006

ORACLE®

Oracle Identity Manager Connector Guide for IBM RACF, Release 9.0.1

B31116-01

Primary Author: Vimmika Dinesh

Contributing Authors: Don Gosselin, Lyju Vadassery

Contents

Preface

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

Note: This is a transitional release following Oracle's acquisition of Thor Technologies. 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 set:

- *Oracle Identity Manager Release Notes*
- *Oracle Identity Manager Installation and Upgrade Guide for JBoss*
- *Oracle Identity Manager Installation and Upgrade Guide for WebLogic*
- *Oracle Identity Manager Installation and Upgrade 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 Connector Framework Guide*
- Connector guides for various third-party applications

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager 9.0.0 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.

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

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

Functionality	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
Installation data Updated	Provisioning	Changes the installation data of a user account. Installation data is one of the fields to be filled in. It can contain any installation/system/project related value.
Operations Updated	Provisioning	Changes the Operations attribute of a user account

Functionality	Type	Description
Special Updated	Provisioning	Changes the Special attribute of a user account in RACF
Auditor Updated	Provisioning	Changes the Auditor attribute of a user account in RACF
Group Access Updated	Provisioning	Changes the Group Access attribute of a user account in RACF
Enables a RACF User	Provisioning	Enables the user on RACF so that the user is able to log in to the IBM Mainframe server, running RACF on z/os
Disables a RACF User	Provisioning	Disables a user on RACF so that the user is not able to log in to the IBM RACF server
Connect Group	Provisioning	Adds a user to a user's group on the IBM RACF server
Disconnect Group	Provisioning	Removes a user from a user's group on the IBM RACF server
Add TSO to a User	Provisioning	Provides TSO(Time Sharing Options) access to a user. TSO is one of the subsystems
Remove TSO	Provisioning	Removes TSO access from a user
Reconcile lookup field	Reconciliation	Reconciles the lookup fields
Reconcile User Data	Reconciliation	Reconciles user data

Reconciliation Module

This section describes the elements that the reconciliation module extracts from the target system to construct a reconciliation event record. In IBM RACF, the reconciliation process can be divided into the following:

- 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 from 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

Name	Description	Data Type
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

Files and Directories That Comprise the Connector

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

`Security Applications\IBM RACF\IBM RACF Rev 1.1.1.zip`

These files and directories are listed in the following table.

File in the Installation Media Directory	Description
`xml\racfResAdp.xml`	This XML file contains records the following Oracle Identity Manager components: ■ IT resource type ■ IT resource ■ Resource object form ■ Process definition ■ Process tasks ■ Connector tasks
`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.

File in the Installation Media Directory	Description
lib\ThirdPartyI\InitialLoginSequence.txt	This file contains the login sequence that the connector function uses to connect to the IBM RACF server. The login sequence provides both the sequence of screens that are displayed while logging in to RACF using IBM Personal Communications and the values to be provided on each screen to proceed further. This should facilitate the connector to reach the READY prompt on the mainframe target server. As TSO is panel driven, after logging in, we do require the cursor to reach a particular prompt.
lib\ThirdParty\logoutSequence.txt	This file contains the logout sequence that the connector function uses to disconnect from the IBM RACF server. The logout sequence provides both the sequence of screens that are displayed while logging off from RACF using IBM Personal Communications and the values to be provided on each screen. This should facilitate the connector to log off from the mainframe target server. As TSO is panel driven, after logging in, we do require the cursor to reach a particular prompt.
xellerate_home\xellerate\ThirdParty\connectionProperties.txt	This file contains the connection parameters and the values of these parameters that are required to connect to the IBM RACF server. This file is used with the troubleshooting utility.
lib\ThirdParty\CustomizedCAs.jar	This file is used for making a secured connection to Mainframe using SSL. It is used to store a copy of SSL certificated installed on the Mainframe Server.
lib\ThirdParty\InputFields.txt	This file contains the connection parameters and the values of these parameters that are required to connect to the IBM Mainframe server. This file is used with the troubleshooting utility.
RACF Scripts\DATAUNLD	This file creates a temporary file and merges the data from SYSTMDAT and JCLSRC, which are part of the code to be deployed on the IBM RACF server, into it 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. DATAUNLD is a member of a procedure library on the IBM RACF server. A procedure library is a Partitioned dataset containing member files.
RACF Scripts\JCLSRC	This file is a template JCL, which is used to submit the background job for use in reconciliation. It is a member of a procedure library on the IBM RACF server. A procedure library is a Partitioned dataset containing member files.
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 RACF server.
RACF Scripts\RXDPTADD	This file uses the temporary file containing the user's department data and adds this information to the user's basic data. It is a member of a procedure library on the IBM RACF server.
RACF Scripts\RXTSOADD	This file uses the temporary file containing the user's TSO data and adds this information to the user's basic data. It is a member of a procedure library on the IBM RACF server.
RACF Scripts\RXGRPADD	This file uses the temporary file containing the user's group privilege and adds this information to the user's basic data. It is a member of a procedure library on the IBM RACF server.
RACF Scripts\RXPRVADD	This file uses the temporary file containing the user's connect privilege data and adds this information to the user's basic data. It is a member of a procedure library on the IBM RACF server.

File in the Installation Media Directory	Description
RACF Scripts\RXPRNTDT	This file uses the temporary file containing the user's data and sends this information to a Java adapter. It is a member of a procedure library on the IBM RACF server.
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 RACF server.
RACF Scripts\RXDIFFER	This file provides differences between old database image and new database image.It is a member of a procedure library on the IBM RACF server.
RACF Scripts\RECNLKUP	This file provides lookup fields data. It is a member of a procedure library on the IBM RACF server.
RACF Scripts\SYSTMDAT	This file is used to provide job configuration parameters to the mainframe system.
troubleshooting\troubleshooting script.txt	This file provides the description of the troubleshooting tool provided with the package.
docs\B31116_01.pdf docs\html	These are PDF and HTML versions of this guide, which provides instructions to deploy the connector.

The "Step 4: Copying External Code" section on page 2-3 provides instructions to copy these files into the required directories.

2

Deploying the Connector

Deploying the connector involves the following steps:

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 systems host platforms	RACF on z/OS 01.04
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`

Step 2: Configuring the Target System

To configure the target system:

1. Create a user on the IBM RACF server.
2. Provide the user with the `special` and `auditor` attributes.

a. Log on to TSO on the IBM RACF server using a user ID with the `Special` attribute.

b. Open the READY prompt, and enter the following command:

```
Altuser NewUserIDCreated Special Auditor
```

3. Set `Msgid` to `ON` for the mainframe user.
4. The **Telnet Services on port specified in IT Resource Type definition** option should be enabled for this particular user to provide network connection between the Oracle Identity Manager server and the IBM RACF server. It's configured as a text description in the TCPIP profile file.
5. **Enable SSL on port if secured connection** is required. It's configured as a text description in the TCPIP profile file.
6. Upload the following members, using FTP, into a partitioned dataset with record length 80 and record format as `Fixed Block`.

Note: Instructions to copy these members into the `RACF Scripts` directory on the Oracle Identity Manager server are given in the "Step 3: Copying the Connector Files" section on page 2-2.

```
DATAEXTT
DATAUNLD
JCLSRC
JOBSTAT
RECNLKUP
RXDIFFER
RXDPTADD
RXGRPADD
RXPRNTDT
RXPRVADD
RXTSOADD
SYSTMDAT
```

7. Upload the following file into a flat file or PS (Physical Sequential file) with record length 80 and record format as `Fixed Block`.

```
xellerate_home\xellerate\RACF Scripts\SYSTMDAT
```

This file should contain the following system-related information, as described in the `systmdat` file:

- IBM RACF database location
- Jobcard, which is for background job, along with the `NOTIFY` parameter
- Location of partitioned dataset consisting of all the scripts
- Region size and dynamic resource allocation values into the script

This file should start with the high-level qualifier of user ID, which carries out reconciliation. For example, it should be referred as *XX*`.SYSTMDAT` where *XX* is the user ID on the IBM RACF server that is used to run reconciliation.

Step 3: 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 Rev 1.1.1.zip`
>
> Refer to "Files and Directories That Comprise the Connector" on page 1-3 for more information about these files.

File in the Installation Media Directory	Destination Directory
`xml\racfResAdp.xml`	*xellerate_home*`\xlclient\`
`lib\JavaTask\xlUtilHostAccess.jar`	*xellerate_home*`\xellerate\JavaTasks`
`lib\ScheduleTask\xlReconRACF.jar`	*xellerate_home*`\xellerate\ScheduleTask`
The following contents of the `lib\ThirdParty` directory: ■ `CustomizedCAs.jar` ■ `InitialLoginSequence.txt` ■ `InputFields.txt` ■ `LogOutSequence.txt`	*xellerate_home*`\xellerate\lib\ThirdParty`
The following contents of the `RACF Scripts` directory: ■ `DATAEXTT` ■ `DATAUNLD` ■ `JCLSRC` ■ `JOBSTAT` ■ `RECNLKUP` ■ `RXDIFFER` ■ `RXDPTADD` ■ `RXGRPADD` ■ `RXPRNTDT` ■ `RXPRVADD` ■ `RXTSOADD` ■ `SYSTMDAT`	*xellerate_home*`\xellerate\RACF Scripts`
`docs\B31117_01.pdf` `docs\html`	*xellerate_home*`\xellerate\docs`

Step 4: 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>
```

IBM Host On-Demand 9.0 (HOD) should be installed to extract APIs as listed in Step 4 in Deployment chapter.

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:

   xellerate_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:

   xellerate_home`\Xellerate\ThirdParty`

Step 5: Importing the Connector XML File

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 *xellerate_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 table in the "Defining IT Resources" section on page 2-5 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. You must remove these nodes. To do this, right-click each such node and then select **Remove.**

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

Defining IT Resources

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

Parameter Name	Parameter Value
Admin	Valid admin ID on the RACF server
AdminCredential	Password of the admin ID account
Application	TSO value to which the admin user logs in. For example, B.
Host	IP address or computer name of the mainframe system
Port	Port number
LoginMacro	This file is used to reach 'Ready' prompt on a Mainframe setup. *xellerate_home*\ThirdParty\loginsequence.txt
AutoRetry	Auto Retry Feature The value can be YES or NO. The default value is NO. **Note**: The values taken by this parameter are case-sensitive.
AmountRetry	Number of retries for AutoRetry feature For example, 2, 5, 10.
WaitTime	Wait time between consecutive retries For example, 10 secs, 20 secs, 30 secs.
IsSecure	Connection secure or not The value can be YES or NO. The default value is NO. **Note**: The values taken by this parameter are case-sensitive.
LogoutMacro	This file is used to exit from 'Ready' prompt on a Mainframe setup. *xellerate_home*\ThirdParty\logoutsequence.txt

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

Step 6: Configuring Reconciliation

Configuring reconciliation involves defining scheduled tasks for Lookup Fields and User reconciliations.

To define the Lookup Fields reconciliation scheduled task, you must specify values for the following attributes of this scheduled task.

Attribute Name	Description	Value
Server	This attribute specifies the IT resource instance that the connector uses to reconcile data.	IT resource instance name for RACF For example, RACF Server.

Attribute Name	Description	Value
LookupField Name	This attribute specifies the name of the lookup field to be reconciled.	Lookup.RACF.Groups Lookup.RACF.Procedures Lookup.RACF.Accounts The values taken by this parameter are case-sensitive.
LookupField Target File	This attribute specifies the name of the file that the connector creates on RACF to temporarily store data.	Valid file name up to 8 characters in length For example, temp, work, temp1, work1
RACF Source Directory	This attribute specifies the RACF directory in which RACF scripts are stored.	RACF directory name For example, ADTTAR.DT250207.CNTL
IsDebug	This attribute specifies whether or not debugging should be performed.	The value can be YES or NO. The default value is NO. **Note**: The values taken by this parameter are case-sensitive.

To define the User reconciliation scheduled task, you must specify values for the following attributes of this scheduled task.

Attribute Name	Description	Value
Target System Recon - Resource Object name	This attribute specifies the name of the resource object.	Resource object name For example, RACF Server
Server	This attribute specifies the IT resource instance that the connector uses to reconcile data.	IT Resource Instance name For example, RACF Server
RACF Source Directory	This attribute specifies the RACF directory in which RACF scripts are stored.	RACF directory name For example, ADTTAR.DT250207.CNTL
Target System New User File	This attribute specifies the name of the file that RACF uses to store the latest image of the RACF database.	Valid file name up to 8 characters in length For example, Recon, Userrecn
Target System Old User File	This attribute specifies the name of the file that RACF uses to store the old image of the RACF database.	Valid file name up to 8 characters in length Reconciling first time, it should be blank. Reconciling Second time, it should be the value used for 'Target System New User File' used for first time reconciliation. Reconciling third time, it should contain the previously used 'Target System Old User File' value.

Attribute Name	Description	Value
IsDebug	This attribute specifies whether or not debugging should be performed.	The value can be YES or NO. The default value is NO. **Note**: The values taken by this parameter are case-sensitive.

Step 7: Compiling Adapters

The following adapters are imported into Oracle Identity Manager when you import the connector XML file. You must compile these adapters before you can use them to provision accounts on the target system.

- adpCREATENEWRACFUSER
- adpRACFUSERDELETE
- adpRACFUSERENABLE
- adpADDTSOTORACFUSER
- adpSETRACFUSERPASSWORD
- adpUPDATERACFUSERATTRIBUTE
- adpCONNECTTOGROUP
- adpDISCONNECTFROMGROUP
- adpREMOVETSO
- adpRACFUSERDISABLE
- adpRACFUPDATEPRIVILEDGE

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 adapters that match the criteria you specified in Step 2.

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 multiple adapters simultaneously, use the Adapter Manager form. To compile one adapter at a time, use the Adapter Factory form. Refer to *Oracle Identity Manager Tools Reference Guide* for information about how to use these forms.

Step 8: Configuring SSL

Note: This step is required only if IsSecure parameter in IT Resource is set to 'YES'.

The IBM RACF connector is capable of establishing a secure SSL connection to the IBM RACF server using a one-way handshake mechanism. SSL uses a cryptographic system that uses two keys to encrypt data: a public key known to everyone and a private or secret key known only to the recipient of the message. As data is encrypted, data integrity is preserved over network.

Configuring Oracle Identity Manager to use SSL connectivity involves the following steps:

1. Set the `IsSecure` parameter of IT resource to `YES`.
2. Configure the target system to enable the required port for SSL connection.
3. Add the certificate in the `CustomizedCAs.p12` file. For more information on adding the certificate in the `CustomizedCAs.p12` file, refer to Adding the Certificate on page 2-8.
4. If the certificate is issued by Thwaite or any other weel-known company, then the `WellKnownTrustedCertificatesCAs.jar` can be prepared and added (refer to the "Step 4: Copying External Code" section on page 2-3).

Adding the Certificate

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 RACF 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 implement the SSL connection to the IBM RACF server through Oracle Identity Manager:

1. Extract the contents of the `CustomizedCAs.jar` file.
2. Add the SSL certificate in the `CustomizedCAs.p12` file.
3. Create the `CustomizedCAs.jar` file with the updated `CustomizedCAs.p12` and `CustomizedCAs.class` files.
4. Copy the updated JAR file into the following directory:

   xellerate_home`\Xellerate\ThirdParty`

3

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected.

> **Note:** In earlier releases of this guide, the connector was referred to as the *integration.*

This chapter contains the following sections:

Running Test Cases

This section discusses test cases that you can perform by using the troubleshooting utility.

You can use the troubleshooting utility to directly use the connector for identifying the cause of problems associated with connecting to the IBM RACF server and performing basic operations on the server. The following are sample test cases that you can run by using the troubleshooting utility.

Open a command window and switch to the directory in which the `xlutilHostAccess.jar` file is present. This file is in the *`xellerate_home`*`\Xellerate\JavaTasks` directory. This utility uses some files from the `ThirdParty` directory.

You can 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
  ```

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

  ```
  java -jar xlUtilHostAccess.jar 2 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

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 to the IBM RACF server	■ Ensure that the IBM RACF server is up and running. ■ Check if the user is not already logged in. ■ Check if the user has been disabled on the IBM RACF server. ■ Check if Oracle Identity Manager is working (that is, the database is running). ■ Ensure that all the adapters have been compiled. ■ Examine the Oracle Identity Manager record (from the IT Resources form). Verify that the IP address, admin ID, and admin password are correct. ■ Check the security parameters if an SSL connection is being used.
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, comma, apostrophe, inverted comma). ■ Ensure that the attribute values do not exceed their permitted lengths.
Reconciliation fails.	Ensure that the file names given to store new user data on IBM RACF do not already exist on the IBM RACF server.

4

Known Issues

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

- The connector does not support trusted system reconciliation.
- Only one TSO set can be attached with a user. If more than one TSO set is provisioned to a single user, then only the last operation 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

Index

T

U

X