

Oracle® Identity Manager

Connector Guide for IBM RACF Advanced,
Release 9.0.1

B31118-01

June 2006

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

Oracle, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Contents

Preface	v
Audience	v
Documentation Accessibility	v
Related Documents	vi
Documentation Updates	vi
Conventions	vi
 1 About the Connector	
Overview of Oracle Identity Manager IBM RACF Advanced Connector	1-1
Supported Functionality	1-2
Provisioning Connector Features	1-2
Reconciliation Features	1-3
Files and Directories That Comprise the Connector	1-3
 2 Installation and Configuration: Part 1	
Step 1: Verifying Deployment Requirements	2-1
Message Transport Layer Requirements	2-1
Step 2: Copying Connector Files	2-2
Step 3: Importing the Connector XML File	2-2
Defining IT Resources	2-3
Step 4: Compiling Adapters	2-3
Step 5: Installing the LDAP Gateway	2-4
Configuring Oracle Identity Manager Gateway for Provisioning	2-5
 3 Installation and Configuration: Part 2	
Step 1: Installation Prerequisites	3-1
Environmental Settings and Requirements	3-1
Step 2: Initiating Connector Installation	3-2
Step 3: Installing the Exits for the Reconciliation Connector	3-3
Step 4: Configuring the Message Transport Layer	3-4
Configuring TCP/IP	3-4
Using MQ Series	3-6
Provisioning Connector Installation for MQ Series	3-6
Reconciliation Connector Installation for MQ series	3-7
Configuration of APF Authorization	3-9

Building and Operation of the Starter Tasks.....	3-10
Batch Loading of ACIDS	3-11

4 Initial Reconciliation Run

5 Testing the Connector

Port Connectivity Testing	5-1
Running Test Cases	5-2
Troubleshooting.....	5-3
Performance Tests	5-4

A Oracle Identity Manager Schema Mappings

B Connector Architecture

Oracle Identity Manager Advanced LDAP Gateway	B-1
Oracle Identity Manager Provisioning Connector.....	B-1
Oracle Identity Manager Reconciliation Connector.....	B-2
Message Transport Layer	B-4

Preface

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

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 Advanced.

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.
<i>italic</i>	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.

About the Connector

The Oracle Identity Manager IBM RACF Advanced Connector provides a native interface into z/OS mainframe and the Oracle Identity Manager. The Advanced Connector functions as a trusted virtual administrator on the targeted platform, performing tasks such as creating login IDs, suspending IDs, changing passwords, and performing other functions that administrators usually perform manually.

The Oracle Identity Manager IBM RACF Advanced Connector enables bi-directional provisioning and reconciliation to IBM RACF security facilities. This chapter also provides an overview of the connector and features of the Advanced Connector.

This chapter discusses the following topics, and provides an overview of the Oracle Identity Manager IBM RACF Advanced Connector components and the supported functionality:

- [Overview of Oracle Identity Manager IBM RACF Advanced Connector](#)
- [Supported Functionality](#)
- [Files and Directories That Comprise the Connector](#)

Overview of Oracle Identity Manager IBM RACF Advanced Connector

The Oracle Identity Manager IBM RACF Advanced Connector includes the following components:

- **Oracle Identity Manager Advanced LDAP Gateway:** The LDAP Gateway receives instructions from the Oracle Identity Manager server in the same way as any LDAP v3 identity store. These LDAP commands are then converted into native mainframe commands for IBM RACF and sent to the Provisioning Connector. The response is also native to IBM RACF, which is then parsed into an LDAP response. After execution, an LDAP-formatted response is returned to the requesting application.
- **Oracle Identity Manager Provisioning Connector:** The Provisioning Connector is a mainframe component, receiving native mainframe IBM RACF provisioning commands from the LDAP Gateway. These requests are processed against the IBM RACF authentication repository with the response parsed and returned to the LDAP Gateway.
- **Oracle Identity Manager Reconciliation Connector:** The Oracle Identity Manager Reconciliation Connector captures native mainframe events using advanced exit technology for seamless bidirectional reconciliation to the Oracle Identity Manager through the LDAP Gateway. The Reconciliation Connector captures events occurring from TSO login, command prompt, batch jobs, and other native events, in real time. The Reconciliation Connector captures these events and transforms

them into notification messages for the Oracle Identity Manager through the LDAP Gateway.

- **Message Transport Layer:** The message transport layer enables the exchange of messages between the LDAP Gateway and the IBM RACF Provisioning and Reconciliation Connector. You can use the following messaging protocols for the message transport layer:
 - IBM MQ Series
 - TCP/IP with internal Advanced Encryption Standard (AES) encryption using 128-bit cryptographic keys. The IBM RACF Advanced connector supports a manually configured message transport layer using the TCP/IP protocol, which is functionally similar to proprietary message transport layer protocols.

In addition, the Advanced connector is engineered for high-performance environments and transactions.

See Also: For more information on the IBM RACF Advanced Connector architecture and configuration of the message transport layer, refer to [Appendix B, "Connector Architecture"](#)

Supported Functionality

The following feature set lists use cases for the Oracle Identity Manager IBM RACF Advanced Connector. It is important to note that the LDAP Gateway receives LDAP v.3 and sends IBM RACF commands to the mainframe through the Provisioning Connector. The return messages are also in IBM RACF format, which are then returned as LDAP v.3 responses.

Provisioning Connector Features

The IBM RACF Advanced connector supports the following provisioning functionality:

- Change RACF Password
- Reset RACF Password
- Create RACF User
- Modify RACF User
- Revoke RACF User Account
- Add user to RACF Group
- Delete RACF User
- Resume RACF User Account
- List RACF Users
- List RACF Groups
- List RACF Users By Group
- List RACF Resource Profiles by User
- Grant RACF User Access to Dataset
- Grant RACF User Access to Resource Profile
- Grant RACF User Access to TSO

Reconciliation Features

The IBM RACF connector provides the following reconciliation functionality:

- Detect and Report Native RACF Password Change Event
- Detect and Report Native RACF Password Reset Event
- Detect and Report Native RACF Create User Data Event
- Detect and Report Native RACF Modify User Data Event
- Detect and Report Native RACF Revoke User Event
- Detect and Report Native RACF Add User to RACF Group Event
- Detect and Report Native RACF Delete User Event
- Detect and Report Native RACF Resume User Event

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 Advanced Rev 1.0.0.zip

The contents of this file are described in brief in the following table:

File or Directory on the Installation Media	Description of Files and Contents
xml\oimRacfConnector.xml	The XML file that contains component definitions for the connector.
lib\idm.jar	The connector JAR file to be deployed on the Oracle Identity Manager system.
etc\LDAP Gateway\	Files required for LDAP Gateway deployment in the distributed environment system.
etc\Provisioning and Reconciliation Connector\Mainframe_RACF\	Files required for Provisioning Connector and Reconciliation Connector Deployment on the mainframe end.
docs\B31116-01.pdf	Oracle Identity Manager Connector Guide for IBM RACF Advanced
docs\html	

Installation and Configuration: Part 1

Deploying the connector in the distributed environment involves the following tasks:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Copying Connector Files](#)
- [Step 3: Importing the Connector XML File](#)
- [Step 4: Compiling Adapters](#)
- [Step 5: Installing the LDAP Gateway](#)

These tasks are performed on the Oracle Identity Manager system where the LDAP Gateway component is installed. The Provisioning and Reconciliation Connectors are installed in the mainframe environment. This is covered in the [Chapter 3, "Installation and Configuration: Part 2"](#).

Step 1: Verifying Deployment Requirements

Verify that the following system requirements are met for deploying the Oracle Identity Manager IBM RACF Advanced Connector. This section describes the platforms, target systems, and versions of Oracle Identity Manager that are compatible with this connector.

Item	Requirement
Oracle Identity Manager Versions	Oracle Identity Manager 8.5.3 or later
Target Systems	IBM RACF Advanced
Target System Host Platform	z/OS IBM Mainframe Supports all z/OS versions
Infrastructure Requirements	Provisioning of the Message Transport Layer of MQ Series or TCP/IP
External Code	N/A
Operating System	Systems that support Java v.1.4.2 or later
Mainframe Repository	IBM z/OS v.1.4, with RACF updated to current patch level
Distributive Environment	Multiplatform Java version 1.4.2 or later

Message Transport Layer Requirements

Between the distributive and mainframe environment, Oracle Identity Manager supports two different secure message transport layers, TCP/IP and IBM MQ Series.

The MQ Series comes with its own internal setup procedures, which are transparent at the LDAP Gateway level. The primary requirement is that port 1414 is used between the Oracle Identity Manager and the mainframe.

Additional configuration is required for the TCP/IP message transport layer. The Oracle Identity Manager reserves the following ports for standard message transport layer communication.

In coordination with an enterprise level architecture, port 5790 is used for the Advanced Provisioning Connector. Between the LDAP Gateway and the Reconciliation Connector, the Oracle Identity Manager reserves ports 5190 through 5199 as a range of ports for multiple LPARs.

The rules for TCP/IP are beyond the scope of this document, but affect the startup and communication sequences. The goal is to establish a stateful connection, allowing the pooling of messages and significantly reducing the load on both the mainframe and the LDAP Gateway server.

- The first step is to start up the Oracle Identity Manager LDAP Gateway. This will have been previously configured to connect to IBM RACF using a given IP address and port number.
- Once the LDAP Gateway is started, start the Provisioning Connector started task, which is also preset to establish the TCP/IP connection to the LDAP Gateway on a specified IP address and port number.
- The same procedure applies to the Reconciliation Connector. Start the LDAP Gateway, and then initiate the Reconciliation Connector started task.

Step 2: Copying Connector Files

Copy the following connector files to the destinations indicated in the following table:

Files	Destination
xml\oimRacfConnector.xml	OIM_HOME\xellerate\XLIntegrations\racf\xml\
lib\idm.jar	OIM_HOME\ xellerate\JavaTasks

Step 3: 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 oimRacfConnector.xml file, which is in the OIM_HOME\xellerate\XLIntegrations\racf\xml\ directory. Details of this XML file are shown on the File Preview page.
5. Click **Add File**. The Substitutions page is displayed.
6. Click **Next**. The Confirmation page is displayed.
7. Click **Next**. The Provide IT Resource Instance Data page for the RacfResource resource is displayed.

8. Specify values for the parameters of the `RacfResource` resource. Refer to the table in the [Defining IT Resources](#) section for information about the values to be specified.
9. Click **Next**. The Provide IT Resource Instance Data page for a new instance of the `RacfResource` 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 file is imported into Oracle Identity Manager.

Defining IT Resources

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

Parameter Name	Parameter Value (Default)
Resource Asset Name	<code>RacfResource</code>
Resource Asset Type	<code>LDAP Server</code>
Admin Id	<code>uid=idfRacfAdmin,ou=People,dc=racf,dc=com</code>
Admin Password	<code>idfRacfPwd</code>
Server Address	<code>localhost</code>
Root DN	<code>dc=racf,dc=com</code>
Port	<code>5389</code>
Is the resource asset to be used to call a method on an API, which resides on a machine that is external to Xellerate?	<code>No</code>

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

Step 4: 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.

- `CreateRacfUser`
- `ChangePassword`
- `ResetPassword`
- `DeleteUser`

-
- RevokeUser
 - ResumeUser
 - ModifyUser
 - GrantTsoAccess
 - AddUserToGroup
 - RemoveUserFromGroup
 - AddUserToDataset
 - RemoveUserFromDataset
 - AddUserToResource
 - RemoveUserFromResource

To compile adapters by using the Adapter Manager form:

1. Open the Adapter Manager form.
2. To compile all the adapters that you have imported 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 you specify.

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 5: Installing the LDAP Gateway

To configure Oracle Identity Manager LDAP Gateway to use the Provisioning functionality:

1. Edit the `run.cmd` or `run.sh` file located under `<install_directory>/bin` directory, set the `JAVA_HOME` variable to match your install Java install directory, and save the file.
 - a. Windows: set `JAVA_HOME=\software\j2sdk1.4.2_08`
 - b. Unix: `JAVA_HOME=/software/j2sdk1.4.2_08`
2. Extract the `oimserver.jar` file and edit the `beans.xml` file located under `<install_directory>/dist/`. Edit the `port` property of the server:

```
<bean id="listener" class=
"com.identityforge.ximserver.nio.Listener">
<constructor-arg><ref bean="bus"/></constructor-arg>
<property name="admin"><value>false</value></property>
```

```

<property name="config"> <value>../conf/listener.xml</value></property>
<property name="port" value="389"/>
</bean>

```

Configuring Oracle Identity Manager Gateway for Provisioning

To configure Oracle Identity Manager LDAP Gateway to use the Provisioning functionality:

1. Open the `ximserver.jar` and edit the `beans.xml` file located under `<install directory>/dist/ximserver.jar`.
2. Find the `<bean name="RACF">` tag and edit the information highlighted in bold in the following code:

```

<bean name="RACF" singleton="true"
class="com.identityforge.ximserver.backend.RACF.RACFModule">

    <!-- The following change is optional. If you make this change, also
         change the metaengine.xml file. -->
    <property name="suffix" value="dc=RACF,dc=com"/>

    <property name="workingDirectory" value="../RACF"/>

    <!-- The following change is optional. -->
    <property name="adminUserDN" value="cn=ximRACFAdmin,dc=RACF,dc=com"/>

    <property name="adminUserPassword" value="ximRACFPwd"/>
    <property name="allowAnonymous" value="true"/>
    <property name="entryCacheSize" value="1000"/>
    <property name="defaultUacc" value="read"/>
    <property name="defaultDelete" value="revoke"/>
    <property name="batchUser" value="false"/>
    <property name="idRules">
        <map>
            <entry key="length" value="7"/>
        </map>
    </property>
    <property name="pwdRules">
        <map>
            <entry key="length" value="8"/>
        </map>
    </property>
    <property name="schema" ref="schemas"/>
    <property name="metaBackend"><ref bean="hpbe"/></property>
    <property name="transport">
        <map>
            <!-- Set to MQ if using IBM MQ Series -->
            <entry key="_type_" value="SOCKET"/>

            <!-- Set to true for 128-bit AES encryption. -->
            <entry key="_isencrypted_" value="false"/>

            <!-- Set to IP of RACF system. -->
            <entry key="_host_" value="64.190.71.35"/>
            <entry key="_port_" value="5790"/>
            <entry key="_qcontext_" value=""/>
            <entry key="_qfactory_" value=""/>
            <entry key="_qname_" value=""/>
            <entry key="_greplyname_" value=""/>
        </map>
    </property>

```

```
</property>
<property name="Connector" value="false"/>
</bean>
```

3. If the domain partition was changed from the default "dc=RACF,dc=com," open up the `metaengine.xml` file located under `<install directory>/conf`.
 - a. Replace all occurrences of the domain partition "dc=RACF,dc=com" with the domain partition that was chosen for your installation.
 - b. Save the file.

Installation and Configuration: Part 2

The Provisioning and Reconciliation Connector Components of the Oracle Identity Manager IBM RACF connector are installed on the mainframe. This chapter describes the installation and configuration of the Oracle Identity Manager Provisioning Connector and Reconciliation Connector in the following sections:

- [Step 1: Installation Prerequisites](#)
- [Step 2: Initiating Connector Installation](#)
- [Step 3: Installing the Exits for the Reconciliation Connector](#)
- [Step 4: Configuring the Message Transport Layer](#)

Step 1: Installation Prerequisites

The following table identifies hardware, software, and authorization prerequisites for the installing Provisioning Connector and Reconciliation Connector.

Item	Requirement
Operating System	z/OS any version
Message Transport Layer	TCP/IP Network MQ Series v.5 or later
z/OS Patch Level	Verify that all current patches are in place.
RACF Identity Repository	Current patch level for z/OS

There are two primary systems that are installed on the mainframe, the Provisioning Connector and the Reconciliation Connector. Both connectors require the installation of a started task and both require placement into an administrative APF authorized library.

Installation of the environment is from load libraries. However, if any environmental issues are encountered, assistance may be needed to quickly diagnose the problem. The following are the toolsets available in a typical mainframe shop to handle these issues:

- **Cobol Compiler:** The current version was compiled using IBM Enterprise COBOL for z/OS and OS/390 3.1.1
- **Assembler:** Oracle Identity Manager currently uses HLASM R4.0.

Environmental Settings and Requirements

The IBM RACF Connectors have the following environment requirements:

- Each Connector uses memory subpools to manage peak load conditions. These subpools require 1.5 to 2.0 MB of mainframe memory for operations.
- The Provisioning Connector program user ID should be given authorization to access subpools on the host platform.
- If MQ Series is used in your environment and you plan for Oracle Identity Manager to use MQ series as a message transport layer, then a sample program that is an MQ-enabled program should be available. An MQ administrator needs to authorize the creation of MQ queues from an automated script.

Oracle Identity Manager requires three queues: a send queue, a receive queue, and a Reconciliation Connector communication queue. The names of these queues will be inserted into the Provisioning Connector and Reconciliation Connector start up JCL.

- If TCP/IP is used in the message transport layer, an administrator must have authorization to create ports on the mainframe, as well as provide security authorizations for the data structures.
- The Reconciliation Connector operates at the Exit level, just outside the mainframe operating system. Typical mainframe shops install custom exits, for example to maintain a certain password format. If there are custom exits already installed, an engineering effort is required to allow Reconciliation Connector exits to coexist with existing exits already deployed. The Oracle Identity Manager exits are engineered to be the last exits called in sequence, allowing existing exits to function normally.
- Installation of new exits within an LPAR may require an IPL of the LPAR.

Step 2: Initiating Connector Installation

These are the initial procedures for installing the components of the Connector on z/OS.

- Transmit or FTP JCL.XMIT and LINKLIB.XMIT to the z/OS server, each with the following specifications RECFM=FB, LRECL=80, BLKSIZE=3120, and DSORG=PS.
- Log in to the z/OS server's TSO environment.
- Expand the CNTL dataset, issue the following command from the ISPF command line:

```
TSO RECEIVE INDA('IDF.CNTL.XMIT')
```

- When prompted to specify restore parameters, enter:

```
DA('IDF.CNTL')
```

- To expand the LINKLIB dataset,, issue the following command from the ISPF command line:

```
TSO RECEIVE INDA('IDF.LINKLIB.XMIT')
```

- When prompted to enter restore parameters, enter:

```
DA('IDF.LINKLIB')
```

- To complete the installation, follow the procedures in IDF.CNTL member #INSTVOY for the Reconciliation Connector components, and member #INSTPIO for the Provisioning Connector component.

Step 3: Installing the Exits for the Reconciliation Connector

Because the exits reside in LPA, an IPL is required to complete the installation. To capture events Reconciliation Connector and its exits should be installed on each LPAR that shares the IBM RACF authentication repository.

Note: The instructions that follow assume you will install both Provisioning Connector and Reconciliation Connector Connectors.

Follow the normal procedure for applying such changes to your z/OS system. It is recommended that you:

- Install and test the exits on a test system or partition first.
- Make a copy of your system volumes before applying any changes.
- Consider packaging the exits as SMP/E user mods.
- Assemble the exits into an authorized load library.

To install the Reconciliation Connector exits:

- Install LOGRIX02, LOGPWX01, and LOGEVX01, the Common Command exits, using the Dynamic Exit Facility.
- For testing, it is recommended that you set up one or more PROGxx members in SYS1.PARMLIB (or equivalent), to allow for easy removal of the exit if desired.
- The following are three commands that will compromise the PARMLIB list you create. The three commands can also be added via operator console commands. Below is a sample command to append the Reconciliation Connector exits to the appropriate IBM RACF exits.

```
EXIT ADD EXITNAME(ICHRIX02) MODULE(LOGRIX02)
EXIT ADD EXITNAME(ICHPWX01) MODULE(LOGPWX01)
EXIT ADD EXITNAME(IRREVX01) MODULE(LOGEVX01)
```

- Copy these three members to your system PARMLIB data set.
- If you already have a PROGAD or PROGDL member, rename the LOG members to a PROGxx name that is not in use.
- When ready, use the console command SET PROG=XX to activate LOGPWX01 as an ICHPWX01 exit point.
- When Ready, use the console command SET PROG=XX to activate LOGRIX02 as an ICHRIX02 exit point.
- When ready, use the console command SET PROG=XX to activate LOGEVX01 as an IRREVX01 exit point.

For permanent installation, do one of the following:

- Add the EXIT ADD statement in PROGAD to your production PROGxx PARMLIB member.
- Add a SET PROG=XX command to CONSOL00 or an automation script, so that it is issued during your IPL procedure.
- Install ICHRIX02, the RACROUTE REQUEST=VERIFY(X) (RACINIT) post processing exit.

Note: If you do not have an existing ICHRIX02 exit, run the job in the samples library member RIX0A. This job uses SMP/E to linkedit LDXRIX02 into SYS1.LPALIB as exit ICHRIX02.

To uninstall the LDX exit, enter SET PROG=XY as a console command or enter the following commands.

```
EXIT DELETE EXITNAME(ICHRIX02) MODULE(LOGRIX02)
EXIT DELETE EXITNAME(ICHPWX01) MODULE(LOGPWX01)
EXIT DELETE EXITNAME(IRREVV01) MODULE(LOGEVX01)
```

To load the exits:

- Command done from the Operator Log (ISPF menu option SDSF then option LOG)

/F LLA,REFRESH
/T PROG=XX Where XX is the Parmlib list name created EX. PROG75
/T PROG=75

To look at the exits:

```
/D PROG,LPA,MODNAME=ICHPWX01
/D PROG,LPA,MODNAME=ICHRIX02
/D PROG,LPA,MODNAME=IRREVV01
```

Sample output of display command.

```
15:47:38 D PROG,LPA,MODNAME=ICHPWX01
15:47:38 CSV550I 15.47.38 LPA DISPLAY 321
15:47:38 FLAGS MODULE ENTRY PT LOAD PT LENGTH DIAG
15:47:38 P ICHPWX01 85024C68 05024C68 00000398 0DA015F8

15:47:38 D PROG,LPA,MODNAME=ICHPWX01
15:47:38 CSV550I 15.47.38 LPA DISPLAY 321
15:47:38 FLAGS MODULE ENTRY PT LOAD PT LENGTH DIAG
15:47:38 P ICHPWX01 85024C68 05024C68 00000398 0DA015F8
```

Step 4: Configuring the Message Transport Layer

This section describes the following Message Transport Layer configuration tasks for both TCP/IP and MQ Series:

- [Configuring TCP/IP](#)
- [Using MQ Series](#)
- [Building and Operation of the Starter Tasks](#)
- [Batch Loading of ACIDS](#)

Configuring TCP/IP

To use TCP/IP for the message transport layer, you need the following IP addresses:

- IP address to be used by z/OS
- IP address for the router
- IP addresses for domain name servers

Using TCP/IP, an administrator will be needed to allow the creation of ports on the mainframe, as well as providing security authorizations for the data structures.

Edit the Provisioning Connector and Reconciliation Connector JCL and make the following changes:

- Insert an installation-approved job card.
- Change the value for PARM=('TCPN=TCPIP' to the name of the running TCP/IP started task).
- Change the IP address to the address of the LPAR (z/OS System that Provisioning Connector will be started from).
- Change the port number to the port assigned in the LPAR (z/OS System that Provisioning Connector will be started from).
- If your installation requires batch feeds then insert the proper VSAMGETU statement. The following code shows the batch loading of RACF ACIDS:

```
//USR98S01 JOB (,xxxxxxx,,'PIONEER UPLOAD PROCESS FOR ACIDS'),
//          'UPLOAD CATS TO XELLTE',
//          REGION=2M,CLASS=6,MSGCLASS=Q,
//          USER=XXXXXXXX,TIME=1440,
//          NOTIFY=&SYSUID,TYPRUN=HOLD
//*
/*ROUTE PRINT CLE
/*
//PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//          PARM=('TCPN=TCPIP',
//          'IPAD=148.141.7.113',
//          'PORT=6500',
//          'DEBUG=Y')
//STEPLIB DD DISP=SHR,DSN=PPRD.IDF.LINKLIB
//          DD DISP=SHR,DSN=SYS2.TCPACCES.V60.LINK
//          DD DISP=SHR,DSN=TCPIP.SEZATCP
//SYSOUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSDBOU DD SYSOUT=*
//SYSABOU DD SYSOUT=*
//ABENDAID DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//VSAMGETU DD DISP=SHR,DSN=LXT99S.FEEDFILE.SORTED
/*
```

If Provisioning Connector is a started task, start Provisioning Connector by issuing "S Pioneer" from the console. If Provisioning Connector is a batch task, submit the Pioneer JCL.

For Reconciliation Connector the Job Control is the same with the exception of the execute card, which is described below:

```
//RECONCILIATION CONNECTORX EXEC PGM=RECONCILIATION CONNECTORX,
// PARM=('TCPN=TCPIP',
//      'IPAD=192.168.1.231',
//      'PORT=5791',
//      'DEBUG=Y')
```

For both Reconciliation Connector and Provisioning Connector the following DEBUG parameter field equivalents can be used:

```
* VALID DEBUG PARMS ARE: N, Y, Z
* N IS FOR NO DEBUGGING OUTPUT
```

-
- * Y IS FOR DEBUGGING OUTPUT
 - * Z IS FOR DEBUGGING OUTPUT, BUT DO NOT WRITE TO MQ.

Note: If you get the "dataset in use" message when attempting to edit a member, use F1 to see who is using the member you are trying to edit. You will have to press F1 twice. The second time will actually give the name of the job using the file that you are trying to edit. You can then go to the z/OS console and remove it by using the p or c command.

Using MQ Series

This section describes the installation of the Provisioning and Reconciliation connectors and configuring them to use IBM MQ Series.

Provisioning Connector Installation for MQ Series

Provisioning Connector uses the following for MQ installation:

- PIONEER: Provisioning Connector start task job control
- PIOCOPY: Copies the Provisioning Connector-started task to your installation procedure library.
- PIODEF: Defines the Provisioning Connector MQ definitions
- PIOMQ: Provisioning Connector MQ definition input

To install the connector, do the following:

1. Edit Member PIONEER.

If using the MQ series protocol:

- Change "QMGR" in the QMGR Parm field to the name of your queue manager.
- Your Queue manager is the actual task name given to the MQ Queue manager in the installing system.
- If desired, enable the debug option by changing Debug=N (the default) to Y.

Caution: This will generate a large amount of output. This should only be done for testing.

- Change `Idf.Linklib` to the name you have given the Oracle Identity Manager Authorized Load Module Library.
2. Edit Member PIOCOPY and submit.
 - Insert your installation approved job card.
 - Change `IDF.CNTL` to the name you have given the Oracle Identity Manager Control Library (The library downloaded in the previous install steps).
 - Change `Sys1.PROCLIB` to the name of the JES PROCLIB you would like to use.
 - Change the Reconciliation Connector-started task to initiate as a started task.
 - Submit PIOCOPY. Ensure that the member VOYAGER is present in your selected JES PROCLIB.

3. For MQ series installations: edit member PIOMQ.

- Change all occurrences of "QMGR" to the name of your queue manager. Your Queue manager is the actual task name given to the MQ Queue manager in the installing system.
- Change all occurrences of "STGCLASS" to the name of the storage class you have chosen for the two Provisioning Connector queues.

Note: For performance reasons, your installation may want to define the two Provisioning Connector queues to different storage classes. If you are using Reconciliation Connector (in addition to Reconciliation Connector), you may want to use separate storage classes for the Reconciliation Connector queue.

4. Edit Member PIDEF and submit.

- Insert your jobcard.
- Change "QMGR" in the parm to the name of your queue manager.
- Change "MQMHLQ" to the high level qualifier of your MQ System datasets.
- Change IDF.CNTL to the name you have given the Oracle Identity Manager control library.
- Submit PIDEF. Ensure that the three objects are defined without errors.

Note: Depending on your security environment, you may need to define Provisioning Connector as a started task and grant access to the dataset and MQ resources.

Provisioning Connector is dependent on MQ series, so ensure that the queue manager is active before starting pioneer.

If Provisioning Connector is a started task, start Provisioning Connector by issuing "S PIONEER" from the console. If Provisioning Connector is a batch task, submit the PIONEER JCL.

Provisioning Connector Is Ready To Start.

Reconciliation Connector Installation for MQ series

The Provisioning Connector installation members distributed in the control library are:

- VOYAGER: VOYAGER Reconciliation Connector-started task job control
- VOYCOPY: Copies the VOYAGER Reconciliation Connector started tasks to the procedure library
- VOYDEF: Defines the Reconciliation Connector MQ definitions
- VOYINIT: Reconciliation Connector initialization-started task
- VOYKILL: Reconciliation Connector subpool removal-started task
- VOYMQ: Reconciliation Connector MQ definition input
- VOYSTOP: Reconciliation Connector stop-started task

Installation instructions:

1. Edit Member VOYAGER.

-
- Change "QMGR" in the QMGR parm field to the name of your queue manager. Your queue manager is the actual task name given to the MQ Queue manager in the installing system.
 - If required, enable the debug option by changing Debug=N to Y.

Caution: This will generate a large amount of output. This should only be performed for testing purposes.

- Change IDF.LINKLIB to the name you have given the Oracle Identity Manager Authorized Load Module Library.
2. Edit Members VOYINIT, VOYKILL, and VOYSTOP.
 - Change IDF.LINKLIB to the name you have given the Oracle Identity Manager Authorized Load Module Library.
 3. Edit Member VOYCOPY and submit.
 - Insert your installation approved job card.
 - Change IDF.CNTL to the name you have given the Oracle Identity Manager control library.
 - Change SYS1PROCLIB to the name of the JESPROCLIB proclib you would like Voyager to be started from as a started task.
 - Submit VOYCOPY.
 - Ensure that members VOYAGER, VOYINIT, VOYKILL, and VOYSTOP are present in selected JES PROCLIB.
 4. Edit Member VOYMQ.
 - Change all occurrences of "QMGR" to the name of your queue manager. Your queue manager is the actual task name given to the MQ Queue manager in the installing system.
 - Change all occurrences of +STGCLASS+ to the name of the storage class you would like the queue for Reconciliation Connector defined.

Note: You may want to assign the Reconciliation Connector to a different storage class than the one used by the Provisioning Connector queues.

5. Edit Member VOYDEF and submit.
 - Insert your job card.
 - Change "QMGR" in the parameter to the name of your queue manager. Your queue manager is the actual task name given to the MQ Queue manager in the installing system.
 - Change +MQMHLQ+ to the high level qualifier of your MQ system datasets.
 - Change IDF.CNTL to the name you have given the Oracle Identity Manager Control Library.
 - Submit VOYDEF. Ensure that the three objects are defined without errors.

Note: Depending on your security environment, you may need to define VOYAGER, VOYINIT, VOYKILL, and VOYSTOP as started tasks and grant access to the dataset and MQ resources.

Reconciliation Connector Is Ready To Start.

- Reconciliation Connector is dependent on MQ. Therefore, ensure that the queue manager is active before starting Voyager.
- Start the VOYINIT task by issuing "S VOYINIT" from the console to create the subpool (This only needs to be done once, unless VOYKILL is run).
- Once VOYINIT ends, then start Reconciliation Connector by issuing "S Voyager" from the console.

Note: To quiesce VOYAGER while leaving the subpool intact, start VOYSTOP by issuing "S VOYSTOP" from the console. To quiesce Reconciliation Connector and destroy the subpool, start VOYKILL by issuing "S VOYKILL" from the console.

Caution: Use of VOYKILL will cause any IBM RACF messages stored in the subpool to be lost.

Configuration of APF Authorization

Create the Necessary Definitions

Note: This step requires that you be appropriately authorized to issue IBM RACF commands and to make alterations to the IBM RACF database. If you do not have the required authority to perform such tasks, you should arrange to enlist the assistance of someone who is qualified to perform these tasks.

- Logon to TSO by using a user ID that has the requisite authority to execute IBM RACF commands and modify the IBM RACF database. For example, IBMUSER normally has such authority.
- From a TSO command line (or Option 6 of ISPF), issue the following IBM RACF command:

```
RDEFINE FACILITY IRR.RADMIN.* UACC(NONE)
```

This command defines a IBM RACF resource named IRR.RADMIN.* in the FACILITY class.

Note: This resource may already be defined to your installation.

- From a TSO command line (or Option 6 of ISPF), issue the following IBM RACF command:

```
PERMIT IRR.RADMIN.* CLASS(FACILITY) ID(STARTER) ACCESS(READ)
```

This command grants READ access to resource `IRR.RADMIN.*` for User ID `STARTER` (this is User ID which the starter task runs under). This allows the starter task to issue RACF commands.

- From a TSO command line (or Option 6 of ISPF), issue the following IBM RACF command:

```
ALTUSER STARTER SPECIAL
```

This command grants the `SPECIAL` attribute to User ID `STARTER`, which allows the started task to access and modify IBM RACF User Profiles.

- Issue the following command from a TSO command line (or Option 6 of ISPF):

```
SETROPTS RACLIST(FACILITY) REFRESH
```

This command updates the in-storage tables of IBM RACF to immediately activate the definitions that you create.

- Once the required IBM RACF definitions are in place, exit to get out of ISPF.

Building and Operation of the Starter Tasks

There are two different JCLs to setup and run Provisioning Connector and Reconciliation Connector. You can use these two JCL files for the basis of a starter task definition.

Note: The JCLs have a time set of 1440 on the jobs.

The parameters for `RUNPIONX.txt` are:

- `TCPN`, the name of the TCP process
- `IPAD`, the IP address of machine that Provisioning Connector is running on
- `PORT`, the port that we are listening on
- `DEBUG`, the debug switch for showing the extra output

The parameters for `RUNVOYAX.txt`

- `TCPN`, the name of the TCP process
- `IPAD`, the IP address of machine that Reconciliation Connector is connection to
- `PORT`, the port that we are talking to
- `DEBUG`, the debug switch for showing the extra output

Source code for each program is:

`RUNPIONx:`

```
//ADCDMPPT JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
// NOTIFY=&SYSUID,REGION=4096K
//PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
// PARM=('TCPN=TCPIP',
//      'IPAD=192.168.1.231',
//      'PORT=5790',
//      'DEBUG=Y')
//STEPLIB DD DISP=SHR,DSN=IDF.LINKLIB
//      DD DISP=SHR,DSN=TCPIP.SEZATCP
//SYSPRINT DD SYSOUT=X
```

```

//SYSUDUMP DD SYSOUT=X
//

RUNVOYAx:

//ADCDMRVX JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
// NOTIFY=&SYSUID,REGION=4096K
//RECONCILIATION CONNECTORX EXEC PGM=RECONCILIATION
CONNECTORX,REGION=0M,TIME=1440,
// PARM=('TCPN=TCPIP',
//      'IPAD=192.168.1.183',
//      'PORT=5190',
//      'DEBUG=Y')
//STEPLIB DD DISP=SHR,DSN=IDF.LINKLIB
//      DD DISP=SHR,DSN=TCPIP.SEZATCP
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//

```

Batch Loading of ACIDS

Pioneer and the LDAP console have the ability to load ACIDs from a file into the conversion process and provision IM product data base records in a set of automated tasks. This facility is useful in loading the new IM system from the existing legacy IBM RACF security database.

This requires the JCL added to the start up task Job Control for Provisioning Connector.

```
//VSAMGETU DD DISP=SHR,DSN=USR99S.FEEDFILE.SORTED
```

The data set name reflects the output of the sort in step 3 below.

The LDAP console will then provide a list of ACIDS for which automated information can be obtained and the new database loaded.

In the `IDF.CNTL` library, you will find a task called `UPLOAD`. The current task is a three-step process. The first step utilizes a IBM RACF utility to create sequential records from the IBM RACF security database. These records do not contain passwords so as to protect the confidential nature of the information. The second step utilizes an IBM utility to extract only the ACID from each record. The third step sorts the ACIDS. This sort is done so that as the ACIDs are fed in and propagated across systems, they are processed sequentially and in proper order to aid the performance of the load process.

Initial Reconciliation Run

After installing the Oracle Identity Manager IBM RACF connector, you need to perform the initial reconciliation of users. This is the process where mainframe users are added to the Oracle Identity Manager to allow extension of enterprise user management of profiles and authorization of resources.

The initialization process is run from the command line on the Oracle Identity Manager server. The command does not require execution at a particular directory path, as long as the Java class path is correctly set.

These commands are:

```
java
-Djava.security.auth.login.config=c:\software\idforacle9.0\xellerate\JavaTasks\Con
fig\auth.conf
com.identityforge.oracle.integration.initial.recon.racf.IdfReconciliationConnector
-X

java
-Djava.security.auth.login.config=c:\software\idforacle9.0\xellerate\JavaTasks\Con
fig\auth.conf
com.identityforge.oracle.integration.initial.recon.racf.IdfReconciliationConnector
-R
```

Note: Please enter these commands on a single line without any line breaks.

These commands and the sample class path can be found in the `intial_load_classpath` file. The controls for these commands are found in the `connection.properties` file.

The following is a sample set of values for these parameters:

```
xlAdminId:xelsysadm
xlAdminPwd:xelsysadm
xlJndiUrl:jnp://192.168.1.120:1099
idfTrusted:true
idfServerUrl:ldap://localhost:5389
idfAdminDn:cn=idfRacfAdmin, dc=racf,dc=com
idfAdminPwd:idfRacfPwd
ouPeople:ou=People
ouGroups:ou=Groups
ouDatasets:ou=Datasets
ouResources:ou=Resources
ouFacilities:ou=Facilities
ouBaseDn:dc=racf,dc=com
```

```
idfSystemAdminDn:cn=Directory Manager, dc=system,dc=backend
idfSystemAdminPwd:testpass
idfSystemDn:dc=system,dc=backend
idfIgnoreIdList:start1,start2,private
idfDoOnlyIdList:martin81,martin82,martin83
idList=do
```

To include or exclude specific users during initial reconciliation, modify the following lines:

```
idfIgnoreIdList:start1,start2,private
idfDoOnlyIdList:martin81,martin82,martin83
```

Note: this control does not support wildcards and is designed for processing or excluding a limited number of users.

Testing the Connector

After you deploy the connector, you must test it to ensure that it functions as expected. The IBM RACF Connector is composed of a Gateway and two mainframe adapters, requiring both connectivity and use cases testing:

This chapter contains information on the the following types of testing:

- **Connectivity testing:** All message transport layers have a dependency on open ports, allowing application data to be to be passed between applications and between machines. This test checks for open ports on the mainframe system from the Oracle Identity Manager system. Within the Oracle Identity Manager Advanced Connector, there are two different message transport layers supported: IBM MQ Series and TCP/IP. Both systems depend on open ports to communicate.
- **Provisioning Testing:** This type of test involves using Oracle Identity Manager for provisioning or de-provisioning one of its users or organizations with a target resource. In other words, Oracle Identity Manager is the starting point of the connector, and the target resource is the end point.
- **Reconciliation Testing:** In this type of test, you reconcile Oracle Identity Manager with either a trusted source or a target resource. In other words, the trusted source or target resource is the starting point of the connector, and Oracle Identity Manager is the end point.

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

This chapter contains the following sections:

- [Port Connectivity Testing](#)
- [Running Test Cases](#)
- [Troubleshooting](#)
- [Performance Tests](#)

Port Connectivity Testing

Within the Oracle Identity Manager Advanced Connector, there are two different message transport layers supported: IBM MQ Series and TCP/IP. Both systems depend on open ports to communicate. This section discusses open port testing for IBM RACF connector. Testing of open ports is done on the Oracle Identity Manager server system.

Note: In enterprise security environments, firewalls may be configured to only allow a ping test from specific machines. Also, please notify your network administrator and the mainframe security manager about the port testing, as this activity may trigger automated network responses and notifications.

The following tests assume that the test will be conducted on the Oracle Identity Manager server, with `localhost` as the IP name of the Oracle Identity Manager server and `[mainframeIP]` as the IP address of the mainframe.

1. Internal to the Oracle Identity Manager server, Oracle Identity Manager and the IBM RACF Advanced Connector communicate on port 5389.

```
ping localhost:5389
```

2. For IBM MQ Series messaging, the standard port is 1414. This port will need to be tested for both the Oracle Identity Manager server and the mainframe system.

```
ping localhost:1414
ping [mainframeIP]:1414
```

3. The TCP/IP message transport layer relies on several different ports. The ports should be matched between each system. For provisioning to IBM RACF, run the following test:

```
ping [mainframeIP]:5791
```

For reconciliation with IBM RACF:

```
ping localhost:5190
ping [mainframeIP]:5190
```

Note: It is common for the mainframe TCP/IP configuration and the IBM RACF Advanced Connector Adapter JCLs to have the same code set, even if multiple LPARs and connectors are used. As the port traffic passes through a router, the public IP address then becomes different from the private locally assigned machine IP address. This conversion of the private and public IP address can also extend to remapping to the ports.

Running Test Cases

This section focuses on the functional and performance test cases that are associated with this connector. The following table includes information on running test cases on the IBM RACF Advanced connector:

Test Case	Test Type	Description/Comment
Test to change IBM RACF Password	Provisioning	A user password is changed, with the change posted to the mainframe through the Advanced Connector.
Test to reset IBM RACF Password	Provisioning	A user password is reset, with the change posted to the mainframe through the Advanced Connector.

Test Case	Test Type	Description/Comment
Test to create IBM RACF User	Provisioning	A user is created, with the change posted to the mainframe through the Advanced Connector.
Test to revoke/disable IBM RACF User Account	Provisioning	A user ID is revoked, with the change posted to the mainframe through the Advanced Connector.
Test to resume IBM RACF User Account	Provisioning	A user ID is resumed from a revoked status, with the change posted to the mainframe through the Advanced Connector.
Test to List IBM RACF Users	Provisioning	A list of users is retrieved from the mainframe IBM RACF repository.
Test to Permit IBM RACF User Access to Resource Profile	Provisioning	A user is authorized to access mainframe resources, with change posted to the mainframe through the Advanced Connector.
Test to permit IBM RACF User Access to TSO	Provisioning	A user is provisioned to log on to the mainframe through TSO, with the change posted to the mainframe through the Advanced Connector.
Test to remove IBM RACF User Access to Dataset	Provisioning	A user is removed from access to a mainframe dataset, with the change posted to the mainframe through the Advanced Connector.
Test to remove IBM RACF User Access to Resource Profile	Provisioning	A user is removed from access to a mainframe resource, with the change posted to the mainframe through the Advanced Connector.
Test to detect and report Native IBM RACF Password Change Event	Reconciliation	A native password change is made on the mainframe and subsequently detected by the Advanced Connector.
Test to detect and report Native IBM RACF Password Reset Event	Reconciliation	A native password reset is made on the mainframe and subsequently detected by the Advanced Connector.
Test to detect and report Native IBM RACF Create User Data Event	Reconciliation	A create user is made by an administrator natively on the mainframe and subsequently detected by the Advanced Connector.
Test to detect and report Native IBM RACF Revoke User Event	Reconciliation	A userID password is revoked through native mainframe events, which is subsequently detected by the Advanced Connector.
Test to detect and report Native IBM RACF Delete User Event	Reconciliation	A userID is deleted through native mainframe events, which is subsequently detected by the Advanced Connector.
Test to detect and report Native IBM RACF Resume User Event	Reconciliation	A userID is resumed from a revoke status through native mainframe events, which is subsequently detected by the Advanced Connector.

Troubleshooting

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

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the IBM RACF Server.	<ul style="list-style-type: none"> ■ Ensure that the mainframe server is up and running. ■ Check that the necessary ports are working. ■ Due to the nature of the Provisioning Adapter, the Gateway must be started first, and then the mainframe JCL started task must be initiated. This is a requirement based on how TCP/IP operates. Check that the server IP which hosts the Gateway is configured in the Reconciliation Connector JCL. ■ View the Gateway logs to determine if messages are being sent or received. ■ Examine the Oracle Identity Manager configuration to verify that the IP address, admin ID, and admin password are correct. ■ Check with the mainframe platform manager to verify that the mainframe user ID and password have not been changed.
The mainframe does not appear to respond.	<ul style="list-style-type: none"> ■ Ensure that the Oracle Identity Manager mappings are correct. ■ Check the configuration mappings for the Advanced Adapter Gateway. ■ Check that the mainframe JCL jobs have not ABENDED. If so, determine the reason for the ABEND and ask the mainframe administrator to restart the jobs.
A particular use case does not appear to be functioning.	<ul style="list-style-type: none"> ■ Check for the use case event in question on the Gateway Server Log. Then check for the event in the specific log assigned to that Advanced Connector. ■ If the event does not register in either of these two logs, investigate the connection between the Oracle Identity Manager and the Advanced Connector Gateway. ■ If the event is in the log but the command has not had the intended change on a mainframe user profile, check for configuration and connections between the Gateway and the mainframe. ■ Check that TCP/IP is turned on or that the IBM MQ series is operational, depending on the particular message transport layer chosen.

Performance Tests

The Oracle Identity Manager IBM RACF Advanced architecture has been engineered for enterprise-level performance. When an identity event passes through an exit, the Reconciliation Connector analyzes the event, and then creates a message, allowing the command to complete its routine without loss of time.

A given event will typically fire multiple exits at the same time. For example, a batch job that generates a password change identity event will fire both a batch exit and a password change exit. The Reconciliation Connector captures both events, filters duplicate entries, and passes the result to the Oracle Identity Manager LDAP Gateway.

A batch job to change 50,000 passwords has been tested on a single LPAR to complete within 10 minutes. Because two exits were involved, 100,000 messages were created, filtered, and transformed into MQ messages. The LDAP Gateway then took 30 minutes to retrieve and update the distributive system identity store, with most of that time consumed by the LDAP database.

The LDAP Gateway is engineered to detect when a given event originates from the Oracle Identity Manager, when it passes through the Reconciliation Connector. Provisioning Connector events also create a native exit event that is detected. To prevent a feedback loop, events that originate from the LDAP Gateway are logged, but are not reported again to the Oracle Identity Manager. By contrast, events that originate outside the Oracle Identity Manager are treated as native events, and recorded for future auditing.

The LDAP Gateway and Reconciliation securely capture, filter, and log the identity events from the host system, publishing them for use by Oracle Identity Manager.

Schema Mappings

The following tables describe the schema used by the Oracle Identity Manager LDAP Gateway.

- [Table A-1, " User Attribute Descriptions"](#)
- [Table A-2, " Group Attribute Descriptions"](#)
- [Table A-3, " Dataset Resource Profile Attribute Descriptions"](#)

Table A-1 User Attribute Descriptions

Oracle Identity Manager Gateway Attribute	RACF Attribute	Description
uid	USER	User's login ID
cn	NAME	User full name
sn	NAME	User last name
givenName	NAME	User first name
userPassword	PASSWORD	Password used to login
attributes	SPECIAL, AUDITOR, GPRACC, OPERATIONS	Attributes for the user
owner	OWNER	The owner of the user's profile
defaultGroup	DEFAULT-GROUP	Default group for the user
instdata	DATA	Installation-defined data for the user
createdate	CREATED	Date user was created
passwordDate	PASSDATE	Date the user's password expires
passwordInterval	PASS-INTERVAL	The number of days a password remains valid for the user
revokeDate	REVOKE DATE	Future date the user will be prevented from accessing the system
resumeDate	RESUME DATE	Future date the user will be allowed access to the system again
memberOf	GROUP	Group information for the user
dataset	MODEL	Dataset profile of the user
lastaccessdate	LAST-ACCESS	Last time the user accessed the system
lastconnectdate	LAST-CONNECT	Last time the user connected

Table A–1 (Continued) User Attribute Descriptions

Oracle Identity Manager Gateway Attribute	RACF Attribute	Description
tsocommand	COMMAND	Command to be run during TSO/E logon
tsodest	DEST	Default SYSOUT destination
tsoseclabel	SECLABEL	User's security label
tsounit	UNIT	Default UNIT name for allocations
tsouserdata	USERDATA	Installation-defined data for the user
tsaacctnum	ACCTNUM	Default TSO account number on the TSO/E logon panel
tsoholdclass	HOLDCLASS	Default hold class
tsojobclass	JOBCLASS	Default job class
tsomaxsize	MAXSIZE	The maximum region size the user can request at logon
tsomsgclass	MSGCLASS	Default message class
tsoproc	PROC	Default logon procedure on the TSO/E logon panel
tsosize	SIZE	Minimum region size if not requested at logon
tsosysoutclass	SYSOUTCLASS	Default SYSOUT class
revoke	NA	Value 'Y' if user is revoked or 'N' if user is resumed
waacnt	WAACNT	Account number for APPC/z/OS processing
waaddr1	WAADDR1	Address line 1 for SYSOUT delivery
waaddr2	WAADDR2	Address line 2 for SYSOUT delivery
waaddr3	WAADDR3	Address line 3 for SYSOUT delivery
waaddr4	WAADDR4	Address line 4 for SYSOUT delivery
wabldg	WABLDG	Building for SYSOUT delivery
wadept	WADEPT	Department for SYSOUT delivery
waname	WANAME	User name for SYSOUT delivery
waroom	WAROOM	Room for SYSOUT delivery

Table A–2 Group Attribute Descriptions

Oracle Identity Manager Attribute	RACF Attribute	Description
cn	GROUP	The group ID
uniqueMember	USERS	The users associated to the group
owner	OWNER	The owner of the group
subgroups	SUBGROUPS	All groups associated with this group
instdata	DATA	The installation data for the group

Table A–3 Dataset Resource Profile Attribute Descriptions

Oracle Identity Manager Attribute	RACF Attribute	Description
cn	PROFILE NAME	The profile id
standardAccessList	ID,ACCESS,ACCESS COUNT	The standard access list of ID and access for the dataset
conditionalAccessList	ID,ACCESSES,ACCESS COUNT	The condition access list of ID and access for the dataset
owner	OWNER	The owner of the dataset
auditing	AUDTING	
notify	NOTIFY	
volumes	VOLUMES,UNIT	
instdata	DATA	The installation data for the dataset

Connector Architecture

This appendix describes the IBM RACF Advanced Connector functionality in detail in the following sections:

- [Oracle Identity Manager Advanced LDAP Gateway](#)
- [Oracle Identity Manager Provisioning Connector](#)
- [Oracle Identity Manager Reconciliation Connector](#)
- [Message Transport Layer](#)

Oracle Identity Manager Advanced LDAP Gateway

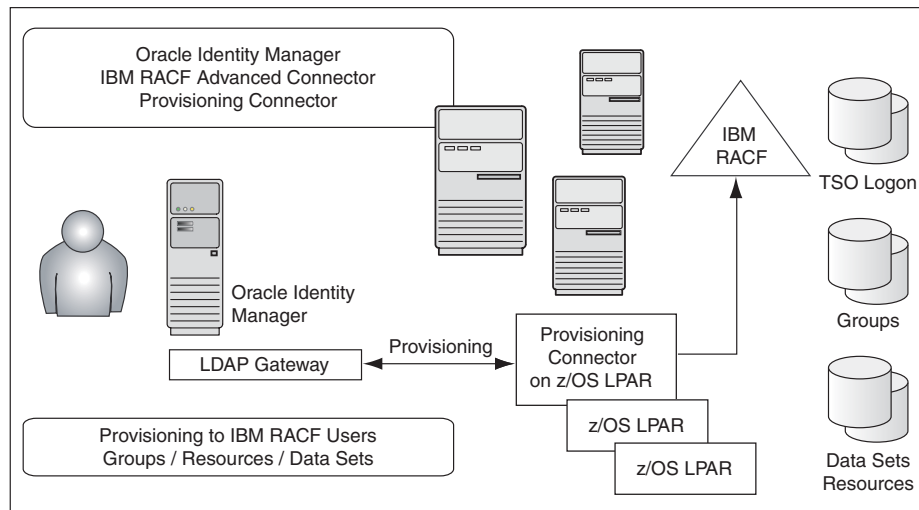
The architecture for Oracle Identity Manager Advanced Connector begins with the Oracle Identity Manager LDAP Gateway. The LDAP Gateway is built on Java 1.4.2, allowing for portability among different platforms and operating systems with complete integration to the Oracle Identity Manager system.

The LDAP Gateway works transparently with Oracle Identity Manager to communicate with IBM RACF Advanced facilities in a z/OS environment. The LDAP Gateway is installed along with the Oracle Identity Manager on the same server. In addition, the Reconciliation Connector enables the LDAP Gateway server to become a subscriber to security and identity events from IBM RACF Advanced.

Oracle Identity Manager maps mainframe authentication repositories by the LDAP DN. By changing the LDAP DN, different authentication repositories and different mainframe resources can be addressed.

Oracle Identity Manager Provisioning Connector

The Provisioning Connector is a mainframe component, receiving native mainframe IBM RACF Advanced provisioning commands from the LDAP Gateway. These requests are processed against the IBM RACF Advanced authentication repository with the response parsed and returned to the LDAP Gateway.



The Provisioning Connector includes LDAP bind and authorization requests. In addition to traditional provisioning functions, the Provisioning Connector can also build the necessary TSO logon functions, including the building CLIST files, and working to replicate existing mainframe user profile scenarios. Provisioning Connector can also extend authorization to data sets, groups, and resources through enterprise rules set in by Oracle Identity Manager.

Internal to mainframe architecture is significant conversation of connector resources and internal mainframe memory subpools for enterprise loads at peak times, supporting over a million transactions per day. The entire Provisioning Connector is protected by AES 128 encryption and APF authorized resources.

The Provisioning connector receives Identity and Authorization change events, and effects requested changes on the z/OS mainframe authentication repository, IBM RACF Advanced. The Provisioning Connector is a mainframe-installed component that receives native mainframe requests from the LDAP Gateway.

An important architectural feature of the Provisioning Connector is that provisioning updates are made from the LDAP Gateway to the IBM RACF Advanced authentication repository. As such, the Provisioning Connector needs to be installed on at least one z/OS LPAR. Provisioning commands sent from the Oracle Identity Manager then change authentication and authorization across all LPARS serviced by the IBM RACF Advanced authentication repository. Within this framework, multiple IBM RACF Advanced systems which are not externally synchronized will require a second Provisioning Connector.

While most provisioning commands are designed around direct access to IBM RACF Advanced, some LDAP provisioning commands are executed in multiple mainframe commands. For example, to provision for TSO access, some systems require modification to a CLIST profile. The type of command depends on which mainframe process is to be accessed.

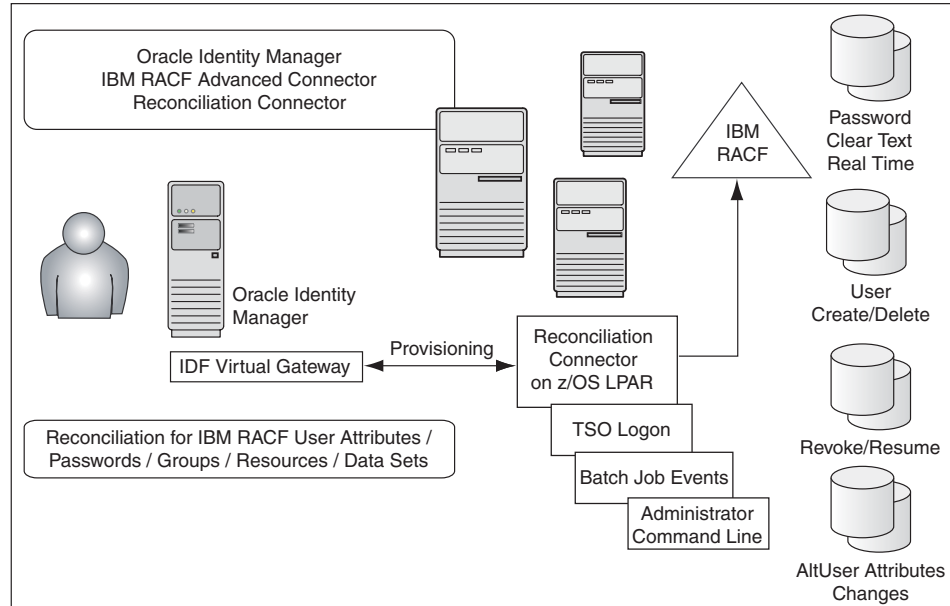
While not within the scope of standard Oracle Identity Management provisioning, the Provisioning Connector can extend control to TSO commands, CICS commands, batch jobs, and other mainframe resources.

Oracle Identity Manager Reconciliation Connector

When an event occurs on the mainframe, independent of any custom installed technology, the event is processed through an appropriate mainframe exit. Because the

Reconciliation Connector uses exit technology, there are no hooks in the z/OS mainframe operating system.

Identity events that arise from a user at TSO login, changes by an administrator from the command prompt, or events resulting from batch jobs are detected and notification messages are securely sent in real time. The Reconciliation Connector captures changes to user attributes (any ALTUSER change), changes to a user account (REVOKE, RESUME), and certain changes to user authorization for groups and resources. If a user account is created or deleted on the mainframe, the Provisioning Connector will notify Oracle Identity Manager and even create a corresponding account in the distributive environment.



Passwords fall into a special category. If business rules permit, a password change will be passed to the Oracle Identity Manager in clear text and real time. In a testing environment, it is almost immediate. Within other business rules, only a notification that the password has been changed will be passed.

Internal to mainframe architecture is significant conversation of connector resources and internal mainframe memory subpools for enterprise loads at peak times. The Reconciliation Connector was specifically designed to handle peak loads from a mainframe batch job. By allocating one meg mainframe memory to the messaging subpools, 50,000 identity event messages can be held as fast as the batch job can produce them (about 8 minutes). These messages are then spooled to the LDAP Gateway, which supplies the messages to the Oracle Identity Manager for subsequent processing (typically over the next hour). The entire Reconciliation Connector is protected by AES 128 encryption and APF authorized resources.

The Reconciliation Connector sends notification events to the Oracle Identity Manager LDAP Gateway from the z/OS mainframe. This architecture does not originate with IBM RACF Advanced, but captures the events just outside the operating system using exit technology, in real time.

A command execution is passed through an exit, just before full completion of the native mainframe command. A common use of this technology is to require user IDs or passwords to be formatted to a proper length or that they must contain at least one letter and one number. If the exit fails, the command fails and returns an error message. By capturing identity or authentication events at an exit, the Reconciliation

Connector captures these events outside the operating system, just prior to completing the command and storing the results in the IBM RACF Advanced authentication repository.

As with the Provisioning Connector, there is an architectural dependence based on the LPAR. When a user ID is created, is authorized to something, or works on the mainframe, they do this on an LPAR. Since all actions are within the LPAR and the Reconciliation Connector detected events from an LPAR exit, the Reconciliation Connector must be installed on each LPAR. This is a scheduled event, usually done with a maintenance schedule, because the an LPAR exit change is only recognized after an IPL.

Message Transport Layer

The message transport layer is the process where the messages are exchanged between the LDAP Gateway and the IBM RACF Advanced Provisioning and Reconciliation Connector.

- IBM MQ Series

Some IBM shops use the IBM MQ Series messaging system as their primary digital communication system. MQ Series is a secure and reliable message transport layer, utilizing internal encryption, conservation of resources, and guaranteed message delivery. The LDAP Gateway supports this message protocol.

- TCP/IP

The LDAP Gateway also uses TCP/IP as a message transport layer to the Provisioning and Reconciliation Connector. This protocol is layered with an internal Advanced Encryption Standard (AES) encryption using 128-bit cryptographic keys. This encryption protocol is internal between the LDAP Gateway and Provisioning / Reconciliation Connector, not depending platform-specific programs or libraries.

The LDAP Gateway, Provisioning Connector, and Reconciliation Connector all coordinate bidirectional synchronization to a single IBM RACF Advanced authentication repository. Internally, the LDAP Gateway has 20 AES cryptographic keys which are randomly selected for a given message, 10 of which are dedicate for bidirectional messages between the Provisioning Connector and the other 10 are used for the Reconciliation Connector.

Messages between the LDAP Connector and the Provisioning Connector have a very short life span. The provisioning process that arises for the Oracle Identity Manager expects a pass or fail LDAP message quickly. Typical logging and auditing protocols exist here and are usually all that are required.

Messages originating from the Reconciliation Connector require the same level of security and guaranteed delivery as MQ Series provides. Within this context, the Reconciliation Connector has been been engineered for the following:

- If the TCP/IP connection has not been established between the Reconciliation Connector and the LDAP Gateway, up to 50,000 messages are kept in a secure mainframe memory subpool prior to message processing.
- During the message generation process, the Reconciliaton Connector places both a time stamp and a sequential serial number to each message. An archive of the message is kept in an encrypted format in an APF authorized VSIM file, with both serial and time/date stamps.

-
- Once transmitted, the messages are logged internally within the LDAP Connector, again in an encrypted format.

Overall, the entire TCP/IP message transport layer approaches the performance and security level of the IBM MQ Series. The Oracle Identity Manager TCP/IP message transport layer is included at no additional charge.

