# Contents

**Preface** ........................................................................................................................................................................... vii
  Audience ........................................................................................................................................................................... vii
  Documentation Accessibility ....................................................................................................................................... vii
  Related Documents ........................................................................................................................................ viii
  Documentation Updates ................................................................................................................................... viii
  Conventions ................................................................................................................................................ viii

1 **About the Connector**

   Overview of Oracle Identity Manager CA ACF2 Advanced Connector .......................................................... 1-1
   Supported Functionality ........................................................................................................................................ 1-2
     Provisioning Connector Functionality ........................................................................................................... 1-2
     Reconciliation Functionality ......................................................................................................................... 1-2
   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: Verifying Installation Requirements .................................................................................................... 3-1
     Environmental Settings and Requirements ..................................................................................................... 3-2
   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 Testing .................................................................................................... 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
Oracle Identity Manager Connector Guide for CA ACF2 Advanced provides information about integrating Oracle Identity Manager with CA ACF2 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 CA ACF2 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/](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:

<table>
<thead>
<tr>
<th>Convention</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>boldface</strong></td>
<td>Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.</td>
</tr>
<tr>
<td>monospace</td>
<td>Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.</td>
</tr>
</tbody>
</table>
The Oracle Identity Manager CA ACF2 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 CA ACF2 Advanced Connector enables bi-directional provisioning and reconciliation to CA ACF2 security facilities. This chapter discusses the following topics, and provides an overview of the Oracle Identity Manager CA ACF2 Advanced Connector components and the supported functionality:

- **Overview of Oracle Identity Manager CA ACF2 Advanced Connector**
- **Supported Functionality**
- **Files and Directories That Comprise the Connector**

### Overview of Oracle Identity Manager CA ACF2 Advanced Connector

The Oracle Identity Manager CA ACF2 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 CA ACF2 and sent to the Provisioning Connector. The response is also native to CA ACF2, 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 CA ACF2 provisioning commands from the LDAP Gateway. These requests are processed against the CA ACF2 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 CA ACF2 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 CA ACF2 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 CA ACF2 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 CA ACF2 Advanced Connector. It is important to note that the LDAP Gateway receives LDAP v.3 and sends CA ACF2 commands to the mainframe through the Provisioning Connector. The return messages are also in CA ACF2 format, which are then returned as LDAP version 3 responses.

#### Provisioning Connector Functionality

The CA ACF2 connector provides the following provisioning functionality:

- Change CA ACF2 Password
- Reset CA ACF2 Password
- Create CA ACF2 User
- Modify CA ACF2 User
- Revoke CA ACF2 User Account
- Add user to CA ACF2 Group
- Delete CA ACF2 User
- Resume CA ACF2 User Account
- List CA ACF2 Users
- List CA ACF2 Groups
- List CA ACF2 Users By Group
- List CA ACF2 Resource Profiles by User
- Grant CA ACF2 User Access to Dataset
- Grant CA ACF2 User Access to Resource Profile
- Grant CA ACF2 User Access to TSO

#### Reconciliation Functionality

The CA ACF2 connector provides the following reconciliation functionality:
- Detect and Report Native CA ACF2 Password Change Event
- Detect and Report Native CA ACF2 Password Reset Event
- Detect and Report Native CA ACF2 Create User Data Event
- Detect and Report Native CA ACF2 Modify User Data Event
- Detect and Report Native CA ACF2 Revoke User Event
- Detect and Report Native CA ACF2 Add User to CA ACF2 Group Event
- Detect and Report Native CA ACF2 Delete User Event
- Detect and Report Native CA ACF2 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:

```text
Security Applications\CA ACF2\CA ACF2 Advanced Rev 1.0.0.zip
```

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

<table>
<thead>
<tr>
<th>Files and Directories</th>
<th>Description of Files and Contents</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>xml\oimAcf2Connector.xml</code></td>
<td>The XML file that contains component definitions for the connector.</td>
</tr>
<tr>
<td><code>lib\idm.jar</code></td>
<td>The connector JAR file to be deployed on the Oracle Identity Manager system.</td>
</tr>
<tr>
<td><code>etc\LDAP Gateway\</code></td>
<td>Files required for LDAP Gateway deployment in the distributed environment system.</td>
</tr>
<tr>
<td><code>etc\Provisioning and Reconciliation Connector\Mainframe_ACF2\directory files</code></td>
<td>Files required for Provisioning Connector and Reconciliation Connector Deployment on the mainframe end.</td>
</tr>
<tr>
<td><code>docs\B31112-01.pdf</code></td>
<td>The CA ACF2 Advanced Connector documentation.</td>
</tr>
<tr>
<td><code>docs\html</code></td>
<td></td>
</tr>
</tbody>
</table>
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 CA ACF2 Advanced Connector.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Identity Manager Versions</td>
<td>Oracle Identity Manager 8.5.3 or later</td>
</tr>
<tr>
<td>Target Systems</td>
<td>CA ACF2 Advanced</td>
</tr>
<tr>
<td>Target Systems Host Platforms</td>
<td>z/OS IBM Mainframe</td>
</tr>
<tr>
<td></td>
<td>Supports all z/OS versions</td>
</tr>
<tr>
<td>Infrastructure Requirements</td>
<td>Provisioning of the Message Transport Layer of MQ Series or TCP/IP</td>
</tr>
<tr>
<td>External Code</td>
<td>N/A</td>
</tr>
<tr>
<td>Operating System</td>
<td>Systems that support Java v.1.4.2 or later</td>
</tr>
<tr>
<td>Mainframe Repository</td>
<td>CA ACF2 Release 6.1, genlevel 9611 or later</td>
</tr>
<tr>
<td>Distributive Environment</td>
<td>Multiplatform Java version 1.4.2 or later</td>
</tr>
</tbody>
</table>

### 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.
Step 2: Copying Connector Files

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

<table>
<thead>
<tr>
<th>Files</th>
<th>Destination</th>
</tr>
</thead>
<tbody>
<tr>
<td>xml\oimAcf2Connector.xml</td>
<td>OIM_HOME\ellerate\XLIntegrations\acf2\xml\</td>
</tr>
<tr>
<td>lib\idm.jar</td>
<td>OIM_HOME\ ellerate\JavaTasks</td>
</tr>
</tbody>
</table>

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 oimAcf2Connector.xml file, which is in the OIM_HOME\ellerate\XLIntegrations\acf2\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 Acf2Resrouce resource is displayed.
8. Specify values for the parameters of the Acf2Resource 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 Acf2Resource 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 Acf2Resource IT resource parameters listed in the following table.

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Parameter Value (Default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Asset Name</td>
<td>Acf2Resource</td>
</tr>
<tr>
<td>Resource Asset Type</td>
<td>LDAP Server</td>
</tr>
<tr>
<td>Admin Id</td>
<td>uid=idfAcf2Admin,ou=People,dc=acf2,dc=com</td>
</tr>
<tr>
<td>Admin Password</td>
<td>idfAcf2Pwd</td>
</tr>
<tr>
<td>Server Address</td>
<td>localhost</td>
</tr>
<tr>
<td>Root DN</td>
<td>dc=acf2,dc=com</td>
</tr>
<tr>
<td>Port</td>
<td>5389</td>
</tr>
</tbody>
</table>

Is the resource asset to be used to call a method on an API, which resides on a machine that is external to Xellerate?

No

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.

- CreateAcf2User
- ResetAcf2Password
- ChangeAcf2UserPassword
- DeleteAcf2User
Step 5: Installing the LDAP Gateway

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 = "ACF2"> tag and edit the properties highlighted in the following code in bold:

```xml
<bean name="ACF2" singleton="true" class="com.identityforge.ximserver.backend.ACF2.ACF2Module">
  <!-- The following change is optional. If you make this change, also edit metaengine.xml -->
  <property name="suffix" value="dc=ACF2,dc=com"/>
  <property name="workingDirectory" value="..ACF2"/>
  <!-- The following change is optional -->
  <property name="adminUserDN" value="oimACF2Admin,dc=ACF2,dc=com"/>
  <property name="adminUserPassword" value="oimACF2Pwd"/>
  <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">
    <!-- For IBM MQ Series set _type_ value to MQ -->
    <entry key="_type_" value="socket"/>
    <!-- Set _isencrypted_ to true for 128-bit AES encryption -->
    <entry key="_isencrypted_" value="false"/>
    <entry key="_host_" value="IPv Address of ACF2 System"/>
    <entry key="_port_" value="5790"/>
    <entry key="_qcontext_" value=""/>
    <entry key="_qfactory_" value=""/>
    <entry key="_qname_" value=""/>
    <entry key="_qreplyname_" value=""/>
  </property>
</bean>
```
3. If the domain partition is changed from the default "dc=ACF2,dc=com", open the metaengine.xml file located at <install directory>/conf.

   a. Replace all occurrences of the domain partition "dc=ACF2,dc=com" with the domain partition that is chosen for your installation.

   b. Save the file.
Installation and Configuration: Part 2

The Provisioning and Reconciliation Connector Components of the Oracle Identity Manager CA ACF2 Advanced 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: Verifying Installation Requirements
- Step 2: Initiating Connector Installation
- Step 3: Installing the Exits for the Reconciliation Connector
- Step 4: Configuring the Message Transport Layer

Step 1: Verifying Installation Requirements

The following table includes hardware, software, and authorization prerequisites for installing both Oracle Identity Manager Provisioning Connector and Oracle Identity Manager Reconciliation Connector.

<table>
<thead>
<tr>
<th>Item</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>z/OS any version</td>
</tr>
<tr>
<td>Message Transport Layer</td>
<td>TCP/IP Network, MQ Series v.5 or later</td>
</tr>
<tr>
<td>z/OS Patch Level</td>
<td>Verify that all current patches are in place.</td>
</tr>
<tr>
<td>CA ACF2 Identity Repository</td>
<td>CA ACF2 Release 6.1, genlevel 9611 or later</td>
</tr>
<tr>
<td></td>
<td>Current patch level for z/OS</td>
</tr>
</tbody>
</table>

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 CA ACF2 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 connectors 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 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')
Step 3: Installing the Exits for the Reconciliation Connector

Because the exits reside in LPA, an IPL is required to complete the installation. To allow the LDAP Gateway to fully capture events, the Reconciliation Connector and its exits should be installed on each LPAR that shares the CA ACF2 authentication repository.

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

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.
- Below 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 CA ACF2 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 the following:
  - LOGPWX01 as an ICHPWX01 exit point
  - LOGRIX02 as an ICHR102 exit point
  - 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.
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

You will need the following IP addresses:

- IP address to be used by z/OS
- IP address for the router

---

**Note:** If you do not have an existing ICHR0X2 exit, run the job in the samples library member RIX0A. This job uses SMP/E to linkedit LDXRIX02 into SYS1.LPALIB as exit ICHR0X2.
Step 4: Configuring the Message Transport Layer

- IP addresses for domain name servers

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

Edit the Provisioning Connector and **VOYAGER JCL** making the following changes:

1. Insert an installation-approved job card.
2. Change the value for **PARAM** from `TCPN=TCPIP` to the name of the running TCP/IP started task.
3. Change the IP address to the address of the LPAR (z/OS System that Provisioning Connector will be started from).
4. Change the port number to the port assigned in the LPAR (z/OS System that Provisioning Connector will be started from).
5. If your installation requires batch feeds then insert the proper **VSAMGETU** statement. The following code illustrates batch loading of CA ACF2 ACIDs:

   ```
   //USR98S01 JOB ('xxxxxxxxx',,'PIONEER UPLOAD PROCESS FOR ACIDS'),
   // 'UPLOAD CATS TO XELLTE',
   // REGION=2M,CLASS=6,MSGCLASS=Q,
   // USER=xxxxxxxxx,TIME=1440,
   // NOTIFY=&SYSUID,TYPRUN=HOLD
   /*
   /*ROUTE PRINT CLE
   /*
   //PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
   // PARM=('TCPN=TCPPIP',
   // '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=* SYSDBOUT DD SYSOUT=* SYSABOUT 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 the `S PIONEER` from the console. If Provisioning Connector is a batch task, submit the **PIONEER JCL**.

For the 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=TCPPIP',
// 'IPAD=192.168.1.231',
// 'PORT=5791',
// 'DEBUG=Y')
```

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

- **N** is for no debugging output.
Step 4: Configuring the Message Transport Layer

- Y is for debugging output.
- Z is for debugging output, but the output is not written to MQ.

**Note:** If you get the "dataset in use" message when attempting to edit a member, use the F1 key to see who is using the member you are trying to edit. You will have to press the F1 key 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 Provisioning and Reconciliation connector installation for MQ series.

#### Provisioning Connector Installation for MQ Series

The 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.
- **PIOMQ:** Provisioning Connector MQ definition input
- **PIODEF:** Defines the Provisioning Connector MQ definitions

To install the connector, do the following:

1. Edit Member PIONEER.
   - a. Change QMGR in the QMGR Parm field to the name of your queue manager.
   - b. Your Queue manager is the actual task name given to the MQ Queue manager in the installing system.
   - c. If desired, enable the debug option by changing `Debug=N` (the default) to `Y`.
   - d. Change IDF.LINKLIB to the name you have given the Oracle Identity Manager Authorized Load Module Library.

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

2. Edit Member Piocopy and submit.
   - a. Insert your installation approved job card.
   - b. Change IDF.CNTL to the name you have given the Oracle Identity Manager Control Library (the library downloaded in the previous install steps).
   - c. Change SYS1.PROCLIB to the name of the JES PROCLIB you would like to use.
   - d. Change the Reconciliation Connector started task to initiate as a started task.
   - e. Submit PIOCOPY. Ensure that the member VOYAGER is present in your selected JES PROCLIB.

3. Edit Member PIOMQ.
Step 4: Configuring the Message Transport Layer

- 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 also using the Reconciliation Connector, you may want to use separate storage classes for the Reconciliation Connector queue.

4. Edit Member PIOMQ 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 PIODEF. 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.

5. Provisioning Connector Is Ready To Start.

**Note:** 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.

---

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

To install the Reconciliation connector, follow these instructions:

1. Edit Member Voyager.
Step 4: Configuring the Message Transport Layer

- 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` & 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.

  Reconciliation Connector Is Ready To Start.
Step 4: Configuring the Message Transport Layer

Installation and Configuration: Part 2

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 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 CA ACF2 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 CA ACF2 commands and to make alterations to the CA ACF2 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.

- Log on to TSO by using a user ID that has the requisite authority to execute CA ACF2 commands and modify the CA ACF2 database. For example, IBMUSER normally has such authority.
- From a TSO command line (or Option 6 of ISPF), issue the following CA ACF2 command:

  RDEFINE FACILITY IRR.RADMIN.* UACC(NONE)

  This command defines a CA ACF2 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 CA ACF2 command:

  PERMIT IRR.RADMIN.* CLASS(FACILITY) ID(STARTER) ACCESS(READ)
Step 4: Configuring the Message Transport Layer

This command grants READ access to the IRR.RADMIN.* resource for the User ID STARTER (the User ID that the starter task runs under). This allows the starter task to issue CA ACF2 commands.

- From a TSO command line (or Option 6 of ISPF), issue the following CA ACF2 command:

  ALTUSER STARTER SPECIAL

  This command grants the SPECIAL attribute to User ID STARTER, which allows the started task to access and modify CA ACF2 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 CA ACF2 to immediately activate the definitions that you create.

- Once the required CA ACF2 definitions are in place, exit from 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
```
Batch Loading of ACIDs

The provisioning connector and the LDAP console have the ability to load ACIDs from a file into the conversion process and provision identity management product database records in a set of automated tasks. This facility is useful in loading the new identity management system from the existing CA ACF2 security database. This requires the JCL added to the start up task Job Control for the Provisioning Connector.

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

The data set name (USR99S) 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 an CA ACF2 utility to create sequential records from the CA ACF2 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.
After installing the Oracle Identity Manager CA ACF2 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\xeellerate\JavaTasks\Config\auth.conf
com.identityforge.oracle.integration.initial.recon.acf2.IdfReconciliationConnector
-X
```

```
java -D
java.security.auth.login.config=c:\software\idforacle9.0\xeellerate\JavaTasks\Config\auth.conf
com.identityforge.oracle.integration.initial.recon.acf2.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 `initial_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:jdbc://192.168.1.120:1099
idfTrusted:true
idfServerUrl:ldap://localhost:5389
idfAdminDn:cn=idfAcf2Admin, dc=acf2,dc=com
idfAdminPwd:idfAcf2Pwd
ouPeople:ou=People
ouGroups:ou=Groups
ouDatasets:ou=Datasets
ouResources:ou=Resources
ouFacilities:ou=Facilities
ouBaseDn:dc=acf2,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.

---
After you deploy the connector, you must test it to ensure that it functions as expected. The CA ACF2 Connector is composed of a Gateway and two mainframe adapters, requiring both connectivity and use cases testing:

This chapter contains information on 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 Testing

**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 CA ACF2 connector. Testing of open ports is done on the Oracle Identity Manager server system.
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 CA ACF2 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 CA ACF2, run the following test:
   
   ping [mainframeIP]:5792

   For reconciliation with CA ACF2:
   
   ping localhost:5290
   ping [mainframeIP]:5290

Note: It is common for the mainframe TCP/IP configuration and the CA ACF2 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 CA ACF2 Advanced connector:

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Test Type</th>
<th>Description/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test to Change CA ACF2</td>
<td>Provisioning</td>
<td>A user password is changed, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Test to Reset CA ACF2</td>
<td>Provisioning</td>
<td>A user password is reset, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Password</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the CA ACF2 connector.

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Test Type</th>
<th>Description/Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test to Create CA ACF2 User</td>
<td>Provisioning</td>
<td>A user is created, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Revoke/disable CA ACF2  User Account</td>
<td>Provisioning</td>
<td>A user ID is revoked, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Resume CA ACF2 User Account</td>
<td>Provisioning</td>
<td>A user ID is resumed from a revoked status, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Test to List CA ACF2 Users</td>
<td>Provisioning</td>
<td>A list of users is retrieved from the mainframe CA ACF2 repository.</td>
</tr>
<tr>
<td>Test to Permit CA ACF2 User Access to Resource Profile</td>
<td>Provisioning</td>
<td>A user is authorized to access mainframe resources, with change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Permit CA ACF2 User Access to TSO</td>
<td>Provisioning</td>
<td>A user is provisioned to logon the mainframe through TSO, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Remove CA ACF2 User Access to Dataset</td>
<td>Provisioning</td>
<td>A user is removed from access to a mainframe dataset, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Remove CA ACF2 User Access to Resource Profile</td>
<td>Provisioning</td>
<td>A user is removed from access to a mainframe resource, with the change posted to the mainframe through the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Detect and Report Native CA ACF2 Password Change Event</td>
<td>Reconciliation</td>
<td>A native password change is made on the mainframe and subsequently detected by the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Detect and Report Native CA ACF2 Password Reset Event</td>
<td>Reconciliation</td>
<td>A native password reset is made on the mainframe and subsequently detected by the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Detect and Report Native CA ACF2 Create User Data Event</td>
<td>Reconciliation</td>
<td>A create user is made by an administrator natively on the mainframe and subsequently detected by the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Detect and Report Native CA ACF2 Revoke User Event</td>
<td>Reconciliation</td>
<td>A userID password is revoked through native mainframe events, which is subsequently detected by the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Detect and Report Native CA ACF2 Delete User Event</td>
<td>Reconciliation</td>
<td>A userID is deleted through native mainframe events, which is subsequently detected by the Advanced Connector.</td>
</tr>
<tr>
<td>Test to Detect and Report Native CA ACF2 Resume User Event</td>
<td>Reconciliation</td>
<td>A userID is resumed from a revoke status through native mainframe events, which is subsequently detected by the Advanced Connector.</td>
</tr>
</tbody>
</table>
### Problem Description | Solution
--- | ---
Oracle Identity Manager cannot establish a connection to the CA ACF2 Server. | ■ 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. | ■ 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. | ■ 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 Testing**

The Oracle Identity Manager CA ACF2 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.
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**

<table>
<thead>
<tr>
<th>Oracle Identity Manager LDAP Gateway Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>User's login user ID</td>
</tr>
<tr>
<td>cn</td>
<td>User full name</td>
</tr>
<tr>
<td>sn</td>
<td>User last name</td>
</tr>
<tr>
<td>givenName</td>
<td>User first name</td>
</tr>
<tr>
<td>userPassword</td>
<td>Password used to login</td>
</tr>
<tr>
<td>attributes</td>
<td>Attributes for the user</td>
</tr>
<tr>
<td>owner</td>
<td>The owner of the user's profile</td>
</tr>
<tr>
<td>defaultGroup</td>
<td>Default group for the user</td>
</tr>
<tr>
<td>instdata</td>
<td>Installation-defined data for the user</td>
</tr>
<tr>
<td>createdate</td>
<td>Date user was created</td>
</tr>
<tr>
<td>passwordDate</td>
<td>Date the user's password expires</td>
</tr>
<tr>
<td>passwordInterval</td>
<td>The number of days a password remains valid for the user</td>
</tr>
<tr>
<td>revokeDate</td>
<td>Future date the user will be prevented from accessing the system</td>
</tr>
<tr>
<td>resumeDate</td>
<td>Future date the user will be allowed access to the system again</td>
</tr>
<tr>
<td>memberOf</td>
<td>Group information for the user</td>
</tr>
<tr>
<td>dataset</td>
<td>Dataset profile of the user</td>
</tr>
<tr>
<td>lastaccessdate</td>
<td>Last time the user accessed the system</td>
</tr>
<tr>
<td>lastconnectdate</td>
<td>Last time the user connected</td>
</tr>
<tr>
<td>tsocommand</td>
<td>Command to be run during TSO/E logon</td>
</tr>
<tr>
<td>tsodest</td>
<td>Default SYSOUT destination</td>
</tr>
</tbody>
</table>
### Table A–2  Group Attribute Descriptions

<table>
<thead>
<tr>
<th>Oracle Identity Manager LDAP Gateway Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>The group ID</td>
</tr>
<tr>
<td>uniqueMember</td>
<td>The users associated to the group</td>
</tr>
<tr>
<td>owner</td>
<td>The owner of the group</td>
</tr>
<tr>
<td>subgroups</td>
<td>All groups associated with this group</td>
</tr>
<tr>
<td>instdata</td>
<td>The installation data for the group</td>
</tr>
</tbody>
</table>

### Table A–3  Dataset Resource Profile Attribute Descriptions

<table>
<thead>
<tr>
<th>Oracle Identity Manager LDAP Gateway Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>The profile id</td>
</tr>
<tr>
<td>standardAccessList</td>
<td>The standard access list of ID and access for the dataset</td>
</tr>
<tr>
<td>conditionalAccessList</td>
<td>The condition access list of ID and access for the dataset</td>
</tr>
<tr>
<td>Oracle Identity Manager LDAP Gateway Attribute</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>owner</td>
<td>The owner of the dataset</td>
</tr>
<tr>
<td>auditing</td>
<td></td>
</tr>
<tr>
<td>notify</td>
<td></td>
</tr>
<tr>
<td>volumes</td>
<td></td>
</tr>
<tr>
<td>instdata</td>
<td>The installation data for the dataset</td>
</tr>
</tbody>
</table>
This appendix describes the CA ACF2 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 CA ACF2 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 CA ACF2.

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 CA ACF2 provisioning commands from the LDAP Gateway. These requests are processed against the CA ACF2 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, CA ACF2. 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 CA ACF2 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 CA ACF2 authentication repository. Within this framework, multiple CA ACF2 systems which are not externally synchronized will require a second Provisioning Connector.

While most provisioning commands are designed around direct access to CA ACF2, 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 CA ACF2, 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 CA ACF2 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 CA ACF2 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 CA ACF2 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 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 Reconciliation 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.