

Oracle® Identity Manager

Connector Guide for CA Top Secret Advanced

Release 9.0.2

B32152-01

September 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
 What's New in the Oracle Identity Manager Connector for CA Top Secret Advanced?	vii
Software Updates	vii
Documentation-Specific Updates.....	viii
 1 About the Connector	
Overview of Oracle Identity Manager CA Top Secret Advanced Connector	1-1
Supported Functionality	1-2
Provisioning Agent Functionality.....	1-2
Reconciliation Agent Functionality	1-2
Multilanguage Support	1-3
Files and Directories That Comprise the Connector	1-3
 2 Deployment and Configuration: Part 1	
Step 1: Verifying Deployment Requirements	2-1
Message Transport Layer Requirements	2-2
Step 2: Copying Connector Files	2-2
Step 3: Configuring the Oracle Identity Manager Server	2-2
Changing to the Input Locale.....	2-3
Clearing the Server Cache.....	2-3
Deploying a Connector on a Clustered Installation of Oracle Identity Manager.....	2-3
Step 4: Importing the Connector XML File	2-4
Defining IT Resources	2-4
Step 5: Compiling Adapters	2-5
Step 6: Installing the LDAP Gateway	2-6
Configuring the LDAP Gateway for Provisioning.....	2-6
Configuring the Connector for Multiple Installations of the Target System	2-7

3 Deployment and Configuration: Part 2

Step 1: Verifying Deployment Requirements	3-1
Environmental Settings	3-2
Step 2: Initial Connector Installation	3-2
Step 3: Installing the Exits for the Reconciliation Agent	3-3
Step 4: Configuring the Message Transport Layer	3-4
TCP/IP Configuration.....	3-4
Using MQ Series.....	3-6
Provisioning Agent Installation for MQ Series.....	3-6
Reconciliation Agent Installation for MQ Series	3-7
Configuration of APF Authorization	3-9
Building and Operation of the Starter Tasks.....	3-10

4 Initial Reconciliation Run

Configuring Trusted Source Reconciliation.....	4-2
--	-----

5 Testing and Troubleshooting

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

6 Known Issues

A Attribute Mapping Between Oracle Identity Manager and CA Top Secret Advanced

B Connector Architecture

Oracle Identity Manager LDAP Gateway	B-1
Oracle Identity Manager Provisioning Agent	B-1
Oracle Identity Manager Reconciliation Agent	B-2
Message Transport Layer	B-4

Index

Preface

Oracle Identity Manager Connector Guide for CA Top Secret Advanced provides information about integrating Oracle Identity Manager with CA Top Secret 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 CA Top Secret Advanced Connector.

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 9.0.2 connector documentation set, visit Oracle Technology Network at

<http://www.oracle.com/technology/documentation/index.html>

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<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.

What's New in the Oracle Identity Manager Connector for CA Top Secret Advanced?

This chapter provides an overview of the updates made to the connector and documentation for CA Top Secret Advanced in release 9.0.2 of the Oracle Identity Manager connector pack.

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

- [Software Updates](#)

These include updates made to the connector software.

- [Documentation-Specific Updates](#)

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

See Also: *Oracle Identity Manager Release Notes*

Software Updates

This section discusses the following software update implemented in this release of the connector.

Incorporation of Multilanguage Support

In addition to English, this release of the connector supports the French and Japanese languages. The following are documentation updates pertaining to the incorporation of this feature:

- The installation media directory includes resource bundle files for the languages supported by the connector. These resource bundle files are described in the [Files and Directories That Comprise the Connector](#) section.
- The [Step 2: Copying Connector Files](#) section provides the destination directory into which you must copy the resource bundle files during the deployment procedure.
- The [Step 3: Configuring the Oracle Identity Manager Server](#) section describes the procedure to change to the required input locale and to clear content related to connector resource bundles from the server cache.
- Two new IT resource parameters have been added to carry country code and language code information to the target system. These parameters are described in the [Defining IT Resources](#) section.

Documentation-Specific Updates

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

- Oracle Identity Manager uses a CA Top Secret user account to connect to and exchange data with CA Top Secret. The [Step 1: Verifying Deployment Requirements](#) section in [Chapter 2](#) provides information about the minimum rights that must be assigned to the Oracle Identity Manager user account. For information on permissions granted to the Provisioning Agent and the Reconciliation Agent, refer to the [Step 1: Verifying Deployment Requirements](#) section in [Chapter 3](#).
- Instructions to copy any connector files and adapter files to all the nodes of a clustered environment have been added in the following sections:
 - [Step 2: Copying Connector Files](#)
 - [Step 5: Compiling Adapters](#)
- Instructions for deploying a connector on a clustered installation of Oracle Identity Manager have been added to [Step 3: Configuring the Oracle Identity Manager Server](#) in [Chapter 2](#).
- Instructions and pointers to information about configuring trusted source reconciliation have been included in the [Configuring Trusted Source Reconciliation](#) section.
- An additional instruction for deploying the LDAP Gateway when using IBM MQ Series for the message transport layer have been included in the [Step 6: Installing the LDAP Gateway](#) section.
- Instructions to configure the connector for multiple installations of CA Top Secret have been added to [Configuring the Connector for Multiple Installations of the Target System](#) in [Chapter 2](#).

About the Connector

The Oracle Identity Manager CA Top Secret Advanced Connector provides an interface between CA Top Secret installed on z/OS mainframe and Oracle Identity Manager. The CA Top Secret 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 Top Secret Advanced Connector enables provisioning and reconciliation to CA Top Secret security facilities. This chapter discusses the following topics:

- [Overview of Oracle Identity Manager CA Top Secret Advanced Connector](#)
- [Supported Functionality](#)
- [Multilanguage Support](#)
- [Files and Directories That Comprise the Connector](#)

Overview of Oracle Identity Manager CA Top Secret Advanced Connector

The Oracle Identity Manager CA Top Secret Advanced Connector includes the following components:

- **LDAP Gateway:** The LDAP Gateway receives instructions from Oracle Identity Manager in the same way as any LDAP version 3 identity store. These LDAP commands are then converted into native mainframe commands for CA Top Secret and sent to the Provisioning Agent. The response is also native to CA Top Secret, which is then parsed into an LDAP response. After execution, an LDAP-formatted response is returned to the requesting application.
- **Provisioning Agent:** The Provisioning Agent is a mainframe component, receiving native mainframe CA Top Secret provisioning commands from the LDAP Gateway. These requests are processed against the CA Top Secret authentication repository with the response parsed and returned to the LDAP Gateway.
- **Reconciliation Agent:** The Oracle Identity Manager Reconciliation Agent captures native mainframe events using advanced exit technology for seamless reconciliation to Oracle Identity Manager through the LDAP Gateway. The Reconciliation Agent captures events occurring from the TSO logins, command prompt, batch jobs, and other native events in real time. The Reconciliation Agent captures these events and transforms them into notification messages for 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 Provisioning and Reconciliation

Agent. 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 Top Secret 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 CA Top Secret Advanced connector is engineered for high-performance environments and transactions.

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

Supported Functionality

The following sections list the functionality available with the Oracle Identity Manager CA Top Secret Advanced Connector.

Provisioning Agent Functionality

The Provisioning Agent provides the following functionality:

- Change passwords
- Reset passwords
- Create users
- Modify users
- Revoke user accounts
- Add user to groups
- Delete users
- Resume user accounts
- List users
- List groups
- List users by groups
- List resource profiles by user
- Grant user access to datasets
- Grant user access to resource profiles
- Grant user access to TSO

Reconciliation Agent Functionality

The Reconciliation Agent provides the following functionality:

- Change passwords
- Password resets
- Create user data

- Modify user data
- Revoke users
- Add users to groups
- Delete users
- Resume users

Multilanguage Support

In addition to English, this release of the connector supports the following languages:

- French
- Japanese

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\CA Top Secret\CA Top Secret Advanced Rev 1.1.0.zip

Extract the contents of this file to the *OIM_HOME* directory. The contents of this file are described in brief in the following table:

Files and Directories	Description of Files and Contents
xml\oimTopsConnector.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 on the Oracle Identity Manager system.
etc\Provisioning and Reconciliation Connector\Mainframe_TS\	Files required for installing the Provisioning Agent and Reconciliation Agent on the mainframe.
Files in the resources directory: <connectorName>.properties <connectorName>_fr.properties <connectorName>_ja.properties	Each of these files contain locale-specific information that is used by the connector.
Files in the docs directory: B32152_01.pdf html	The CA Top Secret Advanced Connector documentation.

See Also: For more information on copying these files to the required destinations for connector deployment, refer to [Chapter 2](#) and [Chapter 3](#).

Deployment and Configuration: Part 1

The CA Top Secret Advanced Connector deployment consists of two parts: the tasks that are performed on the Oracle Identity Manager system and the tasks performed on the mainframe. The deployment procedure on the Oracle Identity Manager system includes installing the LDAP Gateway and is described in the following sections:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Copying Connector Files](#)
- [Step 3: Configuring the Oracle Identity Manager Server](#)
- [Step 4: Importing the Connector XML File](#)
- [Step 5: Compiling Adapters](#)
- [Step 6: Installing the LDAP Gateway](#)
- [Configuring the Connector for Multiple Installations of the Target System](#)

The Provisioning and Reconciliation Agents are installed on the mainframe. This is covered in the [Chapter 3, "Deployment and Configuration: Part 2"](#).

Step 1: Verifying Deployment Requirements

Verify that the following system requirements are met for deploying the Oracle Identity Manager CA Top Secret Advanced Connector. The following table describes the platforms, target systems, and versions of Oracle Identity Manager that are compatible with this connector.

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager 8.5.3 or later
Target Systems	CA Top Secret
Mainframe Repository	CA Top Secret MVS Release 5.0, genlevel 9702 or later
Target Systems Host Platforms	IBM z/OS Mainframe Supports all z/OS versions
Infrastructure Requirements: message transport layer	MQ Series or TCP/IP with AES encryption
Target system user account for Oracle Identity Manager	APF-authorized account with SystemAdministrators privileges

Note: The LDAP Gateway works seamlessly with Oracle Identity Manager and operates under the user account created for Oracle Identity Manager itself. As a result, it has the same permissions as those granted to the Oracle Identity Manager user account to access and operate with the Provisioning Agent and Reconciliation Agent.

Message Transport Layer Requirements

For communication with the mainframe environment, Oracle Identity Manager supports two 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 Oracle Identity Manager and the mainframe.

Additional configuration is required for the TCP/IP message transport layer. 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 Provisioning Agent. Between the LDAP Gateway and the Reconciliation Agent, Oracle Identity Manager reserves ports 5190 through 5199 as a range of ports for multiple LPARs.

Step 2: Copying Connector Files

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

Files in the Installation Media Directory	Destination Directory
xml\oimTopsConnector.xml	OIM_HOME\xellerate\XLIntegrations\tops\xml\
lib\idm.jar	OIM_HOME\xellerate\JavaTasks\
Files in the resources directory: <connectorName>.properties <connectorName>_fr.properties <connectorName>_ja.properties	OIM_HOME\xellerate\connectorResources\
Files in the docs directory: B32152_01.pdf html	OIM_HOME\xellerate\docs\tops

See Also: [Files and Directories That Comprise the Connector](#)

Step 3: Configuring the Oracle Identity Manager Server

- Configuring the Oracle Identity Manager server involves the following procedures:
- [Changing to the Input Locale](#)
 - [Clearing the Server Cache](#)
 - [Deploying a Connector on a Clustered Installation of Oracle Identity Manager](#)

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

Changing to the Input Locale

Configuring the Oracle Identity Manager server involves installing the required fonts and setting the required input locale.

To set the input locale:

1. Open Control Panel.
2. Double-click **Regional Options**.
3. On the Input Locales tab of the Regional Options dialog box, add and switch to the input locale that you want to use.

Clearing the Server Cache

You must clear the server cache whenever you add a new resource bundle file to the `<OIM_home>\xellerate\connectorResources` directory or make a change in an existing resource bundle file.

To clear the server cache:

1. Open a command window, and change to the `<OIM_home>/xellerate/bin` directory.
2. Depending on the operating system, run any one of the following commands:
 - `PurgeCache.bat ConnectorResourceBundle`
 - `PurgeCache.sh ConnectorResourceBundle`

Deploying a Connector on a Clustered Installation of Oracle Identity Manager

Oracle Identity Manager communicates with a mainframe through the advanced LDAP gateway and LPARs. Use the following guidelines to deploy a connector on a clustered installation of Oracle Identity Manager:

- Within the mainframe, multiple LPARs are essentially logical partitions that are tied to a single authentication repository on the mainframe.
- Reconciliation is the detection of an event that occurs against a mainframe authentication repository on an individual LPAR. That event will make a change on the mainframe and affect all attached LPARs. All LPARs where identity events occur should have the the Reconciliation Agent installed and tied to a single LDAP gateway.
- Reconciliation on different sets of mainframe authentication repositories (with each authentication repository having its own set of LPARs) can be directed to different LDAP gateways.
- Provisioning is from the Oracle Identity Manager to the mainframe authentication repository through an LPAR. Since all LPARs attached to the authentication repository will be changed with a provisioning event on a single LPAR, only one LPAR in the group needs to be changed by the LDAP Gateway. If more than one LPAR, in the same group, receives the same change, only the first change will go through and the other changes will give an error because the authentication repository has already been changed.

Some mainframe installations have multiple authentication repositories, but they are all the same type. If the mainframe environment has an internal synchronization process, consult with a mainframe architect or an Oracle Identity Manager Architect on the best way to configure the cluster.

In Release 9.0.2, the CA Top Secret Advanced Connector in a clustered deployment can have only one LDAP Gateway connected to a single mainframe authentication repository (with its attached set of LPARs) in operation at one time. This is a known issue and will be resolved in a future release.

Step 4: 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 `oimTopsConnector.xml` file, which is in the `OIM_HOME\xellerate\XLIntegrations\tops\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 `TopSecretResource` resource is displayed.
8. Specify values for the parameters of the `TopSecretResource` 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 `TopSecretResource` 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 `TopSecretResource` IT resource parameters listed in the following table.

Parameter Name	Parameter Value (Default)
Resource Asset Name	TopSecretResource
Resource Asset Type	LDAP Server
Admin Id	uid=idfTopsAdmin,ou=People,dc=tops,dc=com
Admin Password	idfTopsPwd
Server Address	localhost
Root DN	dc=tops,dc=com
Port	5389
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 5: 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.

- CreateTopsUser
- ResetTopsPassword
- ChangeTopsUserPassword
- DeleteTopsUser
- RevokeTopsUser
- ResumeTopsUser
- GrantTsoTopsUser
- AddTopsUserToGroup
- RemoveTopsUserFromGroup
- AddTopsUserToDataset
- RemoveTopsUserFromDataset
- AddTopsUserToFacility
- RemoveTopsUserFromFacility
- ModifyTopsUser

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.
4. If Oracle Identity Manager is installed in a clustered environment, then copy the compiled adapters from the `OIM_home\xellerate\Adapter` directory to the same directory on each of the other nodes of the cluster. If required, overwrite the adapter files on the other nodes. Then, restart each node.

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 6: Installing the LDAP Gateway

To install the LDAP Gateway, navigate to the `OIM_HOME/etc/LDAP Gateway/` directory (`<LDAP_install_directory>`) and do the following:

1. Edit the `run.cmd` or `run.sh` file located at `<LDAP_install_dir>/bin` directory, set the `JAVA_HOME` variable to match your Java install directory (j2sdk1.4.2 or later), and save the file.
2. Extract the `idfserver.jar` file and edit the `beans.xml` file located under `<LDAP_install_directory>/dist/`. Edit the `port` property of the server and specify the port used for communication between the Gateway and the mainframe LPAR that you use for the connector installation. For example, the port property is set to 5389 in the following code:

```
<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="5389"/>
</bean>
```

3. If you are using IBM MQ Series for the message transport layer, you must copy the following files to the `<LDAP_install_directory>/lib` directory:

- `com.ibm.mq.jar`
- `com.ibm.mqbind.jar`
- `com.ibm.mqjms.jar`
- `fscontext.jar`
- `providerutil.jar`

Configuring the LDAP Gateway for Provisioning

To configure the LDAP Gateway for provisioning:

1. Open the `ximserver.jar` and edit the `beans.xml` file located under `<LDAP_install_directory>/dist/ximserver.jar`.

2. Find the `<bean name="TOPS">` tag and edit the information highlighted in bold in the following code:

```
<bean name="TOPS" singleton="true"
class="com.identityforge.ximserver.backend.TOPS.TopsModule">

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

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

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

    <property name="adminUserPassword" value="ximTOPSPwd" />
    ...
    ...
    <property name="transport">
        <map>
            <!-- 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="Top Secret system IP Address" />
            ...
            ...
        </map>
    </property>
    <property name="Connector" value="false"/>
</bean>
```

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

Configuring the Connector for Multiple Installations of the Target System

Perform the following steps to configure a connector to interface with multiple target system installations:

1. Extract the `beans.xml` file from the `LDAP_install_dir/dist/idfserver.jar` file.
2. Open the `beans.xml` file in a text editor.
3. Locate the `<property name="backends">` and add a `<ref>` element that identifies the identify the name of the Java bean for the target system. For example, the following code configures RACF and TopSecret targets in the same connector:

```
<property name="backends">
    <list>
        <ref bean="hpbe2" />
        <ref bean="racf" />
        <ref bean="tops" />
    </list>
</property>
```

```

    </list>
  </property>

```

4. Locate the `<property name="priority">` and add a `<ref>` element that identifies the priority of each Java bean, as follows:

```

<property name="priority">
  <list>
    <ref bean="be2" />
    <ref bean="be3" />
    <ref bean="be4" />
  </list>
</property>

```

5. Save the beans.xml file and repackage the `LDAP_install_dir/dist/idfserver.jar` file

Deployment and Configuration: Part 2

The Provisioning Agent and Reconciliation Agent components of the Oracle Identity Manager CA Top Secret Advanced Connector are installed on the mainframe.

This chapter describes the installation and configuration of the Provisioning Agent and Reconciliation Agent in the following sections:

- [Step 1: Verifying Deployment Requirements](#)
- [Step 2: Initial Connector Installation](#)
- [Step 3: Installing the Exits for the Reconciliation Agent](#)
- [Step 4: Configuring the Message Transport Layer](#)

Step 1: Verifying Deployment Requirements

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

Item	Requirement
Operating System	IBM z/OS, any version Verify that all current patches are in place.
Message Transport Layer	TCP/IP Network with AES encryption MQ Series v.5 or later
Top Secret Identity Repository	CA-Top Secret MVS Release 5.0, genlevel 9702 or later Current patch level for z/OS
Target system user account for the Provisioning Agent and Reconciliation Agent	APF-authorized user IDs with SystemAdministrators privileges

The Provisioning Agent and the Reconciliation Agent are installed on the mainframe. Both require the installation of a started task. In addition, these agents function under a user ID on the mainframe system. This user ID must be created by the mainframe administrator during the deployment of the Provisioning Agent and the Reconciliation Agent.

Note: Both the Provisioning Agent and Reconciliation Agent user IDs require placement into an administrative APF-authorized library. These user IDs must have at least the permissions of the `SystemAdministrators` group on the mainframe. These permissions are above those of the ordinary administrators on the mainframe, which include Read, Write, Execute, and Modify privileges.

Environmental Settings

The CA Top Secret Advanced connector has the following mainframe environment requirements:

- Each agent uses memory subpools to manage peak load conditions. These subpools require 1.5 to 2.0 MB of mainframe memory for operations. This is configured at the time of installation of the Provisioning and Reconciliation Agents.
- In addition to the program itself, the user ID that a program runs under must also have authorization to access subpools on the host platform. This is typically configured by the mainframe administrator.
- If MQ Series is used for the message transport layer, an MQ administrator will be needed to authorize the creation of MQ queues from an automated script that comes with the connector.

Oracle Identity Manager requires three queues: a send queue, a receive queue, and a communication queue for the Reconciliation Agent. The MQ administrator creates these queues and typically names them according to the naming conventions used in the system. These names are automatically inserted into the Provisioning Agent and Reconciliation Agent start up Job Control Language (JCL) program.

- 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.
- The Reconciliation Agent operates using user exit technology, outside the mainframe operating system. This means it runs in a different LPAR from the operating system.

Typical mainframe shops install custom exits, for example to maintain a certain password format. Oracle Identity Manager exits are engineered to be the last exits called in sequence, allowing existing exits to function normally. After modifying exits within a logical partition (LPAR), an initial program load (IPL) of the LPAR may be required.

Step 2: Initial Connector Installation

These are the initial steps for installing the components of the CA Top Secret Advanced connector on z/OS.

1. 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`.
2. Log in to the z/OS server TSO environment.
3. Expand the CNTL dataset, issue the following command from the ISPF command line:

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

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

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

5. When prompted to enter restore parameters, enter:

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

6. To complete the installation, follow the procedures in IDF.CNTL member #INSTVOY for the Reconciliation Agent, and member #INSTPIO for the Provisioning Agent.

Step 3: Installing the Exits for the Reconciliation Agent

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

Follow the normal procedure for installing exits on the z/OS system. To install the Reconciliation Agent exits:

1. Install LOGRIX02, LOGPWX01, and LOGEVX01, the Common Command exits, using the Dynamic Exit Facility.
2. 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.
3. The following commands comprise the PARMLIB list. These commands can also be added with operator console commands. The following sample command is used to append the Reconciliation Agent exits to the appropriate CA Top Secret exits:

```
EXIT ADD EXITNAME(ICHRIX02) MODULE(LOGRIX02)
EXIT ADD EXITNAME(ICHPWX01) MODULE(LOGPWX01)
EXIT ADD EXITNAME(IRREVS01) MODULE(LOGEVX01)
```

4. 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.
5. When ready, use the console command SET PROG=XX to activate LOGPWX01 as an ICHPWX01 exit point.
6. When Ready, use the console command SET PROG=XX to activate LOGRIX02 as an ICHRIX02 exit point.
7. When ready, use the console command SET PROG=XX to activate LOGEVX01 as an IRREVS01 exit point.

Permanent Installation

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.

Loading the Exits

To load the exits, use the following command 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
```

Viewing the Exits

To view the exits:

```
/D PROG,LPA,MODNAME=ICHPWX01
/D PROG,LPA,MODNAME=ICHRIX02
/D PROG,LPA,MODNAME=IRREVX01
```

Sample output of the 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
```

Uninstalling the Exits

To uninstall the Reconciliation Agent exits, 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(IRREVX01) MODULE(LOGEVX01)
```

Step 4: Configuring the Message Transport Layer

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

- [TCP/IP Configuration](#)
- [Using MQ Series](#)
- [Building and Operation of the Starter Tasks](#)

TCP/IP Configuration

The rules for using 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.

1. The first step is to start up the Oracle Identity Manager LDAP Gateway. This will have been previously configured to connect to using a given IP address and port number.
2. Once the LDAP Gateway is started, start the Provisioning Agent 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 Agent. Start the LDAP Gateway, and then initiate the Reconciliation Agent started task.

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

For 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 Agent and Reconciliation Agent JCL making the following changes:

1. Insert an installation-approved job card.
2. Change the value for PARM= ('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 Agent will be started from).
4. Change the port number to the port assigned in the LPAR (z/OS System that Provisioning Agent will be started from).
5. If your installation requires batch feeds then insert the proper VSAMGETU statement.

```
//USR98S01 JOB (,xxxxxxx,,'PROVISIONING AGENT UPLOAD PROCESS FOR ACIDS'),
//          'UPLOAD CATS TO XELLTE',
//          REGION=2M,CLASS=6,MSGCLASS=Q,
//          USER=xxxxxxx,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=*
//SYSDOUT DD SYSOUT=*
//SYSABOUT DD SYSOUT=*
//ABENDAID DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//VSAMGETU DD DISP=SHR,DSN=LXT99S.FEEDFILE.SORTED
/*
```

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

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

For both Reconciliation Agent and Provisioning Agent, 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 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 Agent installation for MQ series.

Provisioning Agent Installation for MQ Series

Provisioning Agent uses the following members for MQ installation:

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

To install the Provisioning Agent, do the following:

1. Edit member PIONEER.
 - a. 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 system.
 - b. If required, enable the debug option by setting Debug=N (the default) to Y.

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

- c. Change IDF.LINKLIB to the name you have given the Oracle Identity Manager Authorized Load Module Library.
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. See [Step 2: Initial Connector Installation](#)
 - c. Change `SYS1.PROCLIB` to the name of the JES `PROCLIB` you would like to use.
 - d. Change the Reconciliation Agent-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`.
 - a. 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 installation.
 - b. Change all occurrences of "STGCLASS" to the name of the storage class for the two Provisioning Agent queues.

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

4. Edit member `PIODEF` and submit.
 - a. Insert your job card.
 - b. Change "QMGR" in the PARM to the name of your queue manager.
 - c. Change "MQMHLQ" to the high level qualifier of your MQ System datasets.
 - d. Change `IDF.CNTL` to the name you have given the Oracle Identity Manager Control Library.

Provisioning Agent is ready to start.

Note: Provisioning Agent is dependent on MQ series, so ensure that the queue manager is active before starting the Provisioning Agent.

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

Reconciliation Agent Installation for MQ Series

The Reconciliation Agent installation members in the control library are:

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

- VOYSTOP: Reconciliation Agent stop started task

Installation instructions:

1. Edit member VOYAGER.
 - a. 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 installation.
 - b. 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.

- c. 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.
 - a. Insert your installation approved job card.
 - b. Change IDF.CNTL to the name you have given the Oracle Identity Manager Control Library.
 - c. Change SYS1.PROCLIB to the name of the JES PROCLIB you would like the Reconciliation Agent to be started from as a started task.
 - d. Ensure that members VOYAGER, VOYINIT, VOYKILL, and VOYSTOP are present in selected JES PROCLIB.
4. For installations with MQ Series: edit member VOYMQ.
 - a. 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 installation.
 - b. Change all occurrences of +STGCLASS+ to the name of the storage class for Reconciliation Agent queue.

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

5. Edit member VOYDEF and submit.
 - a. Insert your job card.
 - b. 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 installation.
 - c. Change +MQMHLQ+ to the high level qualifier of your MQ system datasets.
 - d. Change IDF.CNTL to the name you have given the Oracle Identity Manager Control Library.
 - e. 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 Agent is ready to start.

Additional Notes

- Reconciliation Agent is dependent on MQ. Therefore, ensure that the queue manager is active before starting the Reconciliation Agent.
- 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 Agent by issuing "S VOYAGER" from the console.
- To quiesce VOYAGER while leaving the subpool intact, start VOYSTOP by issuing "S VOYSTOP" from the console. To quiesce Reconciliation Agent and destroy the subpool, start VOYKILL by issuing "S VOYKILL" from the console. Use of VOYKILL will cause any messages stored in the subpool to be lost.

Note: Events detected by the Reconciliation Agent through exit technology are transformed into messages and passed to the LDAP Gateway.

If MQ Series is used as the message transport layer, these messages are secured internally within the MQ system for delivery.

If the TCP/IP message transport layer is used, the messages are securely sent to the Gateway. If the Gateway is down, messages are held until the Gateway is returned to service, but also secured in an AES encrypted file on the mainframe. When the Gateway resumes, the messages are then sent.

If the subpool is stopped by an administrator, it shuts down the Provisioning Agent, destroying any messages not transmitted. However, the messages in the secured AES-encrypted file are not affected and can be recovered.

Configuration of APF Authorization

APF stands for the IBM Authorized Program Facility. Granting a program the APF Authorized status is similar to giving superuser status. This process will allow a program to run without allowing normal system administrators to query or interfere with its operation. Both the program that runs on the mainframe system and the user ID it runs under must have APF authorization. For example, both the Provisioning Agent program user ID must also have APF authorization.

Note: APF authorization is usually done by a mainframe administrator. 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.

For APF authorization, you need to create the necessary definitions.

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

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

This command defines a resource named `IRR.RADMIN.*` in the `FACILITY` class.
- From a TSO command line (or Option 6 of ISPF), issue the following command:

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

This command grants `READ` access to resource `IRR.RADMIN.*` for User ID `STARTER` (an example of the User ID of the starter task). This allows the starter task to issue commands.
- From a TSO command line (or Option 6 of ISPF), issue the following command:

```
ALTUSER STARTER SPECIAL
```

This command grants the `SPECIAL` attribute to User ID `STARTER`, which allows the started task to access and modify 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 to immediately activate the definitions that you create.
- Once the required definitions are in place, exit to get out of ISPF.

Building and Operation of the Starter Tasks

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

The parameters for `RUNPIONX.txt` are:

- `TCPN`, the name of the TCP process
- `IPAD`, the IP address of the machine that the Provisioning Agent is running on
- `PORT`, the incoming connection port for the Provisioning Agent
- `DEBUG`, the debug switch for showing the extra output

The parameters for `RUNVOYAX.txt` are:

- `TCPN`, the name of the TCP process
- `IPAD`, the IP address of the machine that the Reconciliation Agent is connected to
- `PORT`, the outgoing connection port for the Reconciliation Agent
- `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
//VOYAGERX EXEC PGM=VOYAGERX,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
//
```

Initial Reconciliation Run

After installing Oracle Identity Manager and the connector, you need to perform the initial reconciliation of users. This is the process where mainframe users are added to 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=
OIM_HOME\xellerate\JavaTasks\Config\auth.conf
com.identityforge.oracle.integration.initial.recon.tops.IdfReconciliationConnector
-X
```

```
java -Djava.security.auth.login.config=
OIM_HOME\xellerate\JavaTasks\Config\auth.conf
com.identityforge.oracle.integration.initial.recon.tops.IdfReconciliationConnector
-R
```

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

These commands and a 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=idfTopsAdmin, dc=tops,dc=com
idfAdminPwd:idfTopsPwd
ouPeople:ou=People
ouGroups:ou=Groups
ouDatasets:ou=Datasets
ouResources:ou=Resources
ouFacilities:ou=Facilities
ouBaseDn:dc=tops,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:jdoe81,jdoe82,jdoe83
```

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

Configuring Trusted Source Reconciliation

To configure the connector to perform trusted source reconciliation, set the `idfTrusted` control in the `connection.properties` file to `true`, as follows:

```
idfTrusted:true
```

This control toggles trusted source reconciliation in the connector. Set this to `false` if you are not performing reconciliation with a trusted source.

Note: Reconciliation updates to Oracle Identity Manager are in real-time, and you do not need to configure reconciliation as a scheduled task on Oracle Identity Manager.

Refer to *Oracle Identity Manager Connector Framework Guide* for conceptual information about reconciliation configurations.

Testing and Troubleshooting

After you deploy the connector, you must test it to ensure that it functions as expected. 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 passed between applications and between machines. This test checks for open ports on the mainframe system from the Oracle Identity Manager system. Both IBM MQ Series and TCP/IP 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 the target resource. In other words, the 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

This section discusses open port testing for the 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 computers. Also, you must notify your network administrator and the mainframe security manager about the port testing, because this activity might 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. 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
```

2. The TCP/IP message transport layer relies on several different ports. The ports should be matched between each system. For provisioning to CA Top Secret Advanced, run the following test:

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

For reconciliation with CA Top Secret Advanced:

```
ping localhost:5390
ping [mainframeIP]:5390
```

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

Test Case	Test Type	Description/Comment
Test to change CA Top Secret Advanced Password	Provisioning	A user password is changed, with the change posted to the mainframe through the connector.
Test to reset CA Top Secret Advanced Password	Provisioning	A user password is reset, with the change posted to the mainframe through the connector.
Test to create CA Top Secret Advanced User	Provisioning	A user is created, with the change posted to the mainframe through the connector.
Test to revoke/disable CA Top Secret Advanced User Account	Provisioning	A user ID is revoked, with the change posted to the mainframe through the connector.
Test to resume CA Top Secret Advanced User Account	Provisioning	A user ID is resumed from a revoked status, with the change posted to the mainframe through the connector.
Test to List CA Top Secret Advanced Users	Provisioning	A list of users is retrieved from the mainframe repository.
Test to Permit CA Top Secret Advanced User Access to Resource Profile	Provisioning	A user is authorized to access mainframe resources, with change posted to the mainframe through the connector.

Test Case	Test Type	Description/Comment
Test to permit CA Top Secret Advanced 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 connector.
Test to remove CA Top Secret Advanced User Access to Dataset	Provisioning	A user is removed from access to a mainframe dataset, with the change posted to the mainframe through the connector.
Test to remove CA Top Secret Advanced 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 connector.
Test to detect and report Native CA Top Secret Advanced Password Change Event	Reconciliation	A native password change is made on the mainframe and subsequently detected by the connector.
Test to detect and report Native CA Top Secret Advanced Password Reset Event	Reconciliation	A native password reset is made on the mainframe and subsequently detected by the connector.
Test to detect and report Native CA Top Secret Advanced Create User Data Event	Reconciliation	User creation is done by an administrator natively on the mainframe and subsequently detected by the connector.
Test to detect and report Native CA Top Secret Advanced Revoke User Event	Reconciliation	A user ID password is revoked through native mainframe events, which is subsequently detected by the connector.
Test to detect and report Native CA Top Secret Advanced Delete User Event	Reconciliation	A user ID is deleted through native mainframe events, which is subsequently detected by the connector.
Test to detect and report Native CA Top Secret Advanced Resume User Event	Reconciliation	A user ID is resumed from a revoke status through native mainframe events, which is subsequently detected by the connector.

Troubleshooting

The following table lists solutions to some commonly encountered issues associated with the CA Top Secret Advanced Connector.

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the CA Top Secret Advanced 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 Agent, 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 Agent 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 LDAP 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 CA Top Secret Advanced Connector. ■ If the event does not register in either of these two logs, investigate the connection between the Oracle Identity Manager and the CA Top Secret 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 CA Top Secret Advanced Connector architecture has been engineered for enterprise-level performance. When an identity event passes through an exit, the Reconciliation Agent 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 Agent 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 Oracle Identity Manager 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 Oracle Identity Manager, when it passes through the Reconciliation Agent. Provisioning Agent 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 Oracle Identity Manager. By contrast, events that originate outside 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.

Known Issues

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

- The Oracle Identity Manager CA Top Secret Advanced Connector can accept and transmit any non-ASCII data to the mainframe, but the mainframe does not accept non-ASCII characters. As a result, any task that requires non-ASCII data transfer fails. In addition, there is no provision in the connector to indicate that the task has failed or that an error has occurred on the mainframe. You must exercise caution when providing inputs to the connector for the target system, especially when using a regional language interface.
- Passwords used on the mainframe must conform to stringent rules about passwords on mainframes. These passwords are also subject to restrictions imposed by corporate policies and rules about mainframe passwords. While creating user accounts for target systems on the mainframe, you must take these requirements into account before assigning passwords for these accounts.
- This only applies to a configuration where a single LDAP Gateway connects to multiple installations of the target system. If you configure the connector for trusted source reconciliation and set the `idfTrusted` parameter to true in one of the target system installations on the mainframe, then it must be set to true in all installations that connect to the same Gateway. Otherwise, the connector will fail to work.
- Release 8.2x version of the connector is not localized for the French and Japanese languages. For this release of the connector, the connector-related fields in Oracle Identity Manager can be displayed only in English.

Attribute Mapping Between Oracle Identity Manager and CA Top Secret Advanced

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	Top Secret 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

Table A–1 (Cont.) User Attribute Descriptions

Oracle Identity Manager Gateway Attribute	Top Secret Attribute	Description
lastconnectdate	LAST-CONNECT	Last time the user connected
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
tsjobclass	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
waacct	WAACCT	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	Top Secret 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	Top Secret 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,ACCESS,ACCESS COUNT	The condition access list of ID and access for the dataset
owner	OWNER	The owner of the dataset
auditing	AUDITING	Indicates whether auditing should be enabled
notify	NOTIFY	Indicates whether notification is enabled for any changes to resource profiles
instdata	DATA	The installation data for the dataset

Connector Architecture

This appendix describes the CA Top Secret Advanced Connector functionality in detail in the following sections:

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

Oracle Identity Manager LDAP Gateway

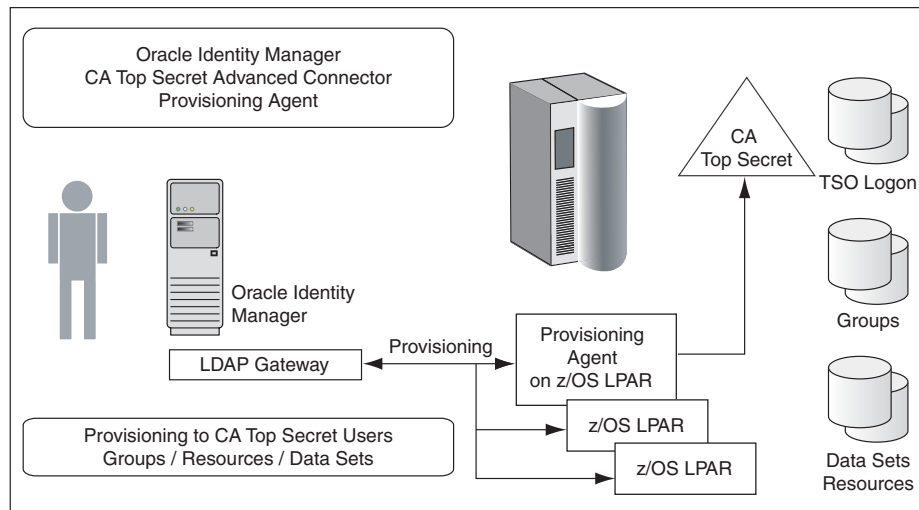
The architecture for Oracle Identity Manager CA Top Secret Advanced Connector begins with the Oracle Identity Manager LDAP Gateway. The LDAP Gateway is built on Java 1.4.2, allowing for portability across different platforms and operating systems and complete integration with the Oracle Identity Manager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

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

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 Agent

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



The Provisioning Agent includes LDAP bind and authorization requests. In addition to traditional provisioning functions, the Provisioning Agent can also build the necessary TSO logon functions, including the building CLIST files, and working to replicate existing mainframe user profile scenarios. Provisioning Agent 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 communication of connector resources and internal mainframe memory subpools for enterprise loads at peak times, supporting over a million transactions per day. The entire Provisioning Agent is protected by AES 128 encryption and APF authorized resources.

The Provisioning Agent receives Identity and Authorization change events, and effects requested changes on the z/OS mainframe authentication repository, CA Top Secret. The Provisioning Agent is a mainframe-installed component that receives native mainframe requests from the LDAP Gateway.

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

While most provisioning commands are designed around direct access to CA Top Secret, 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.

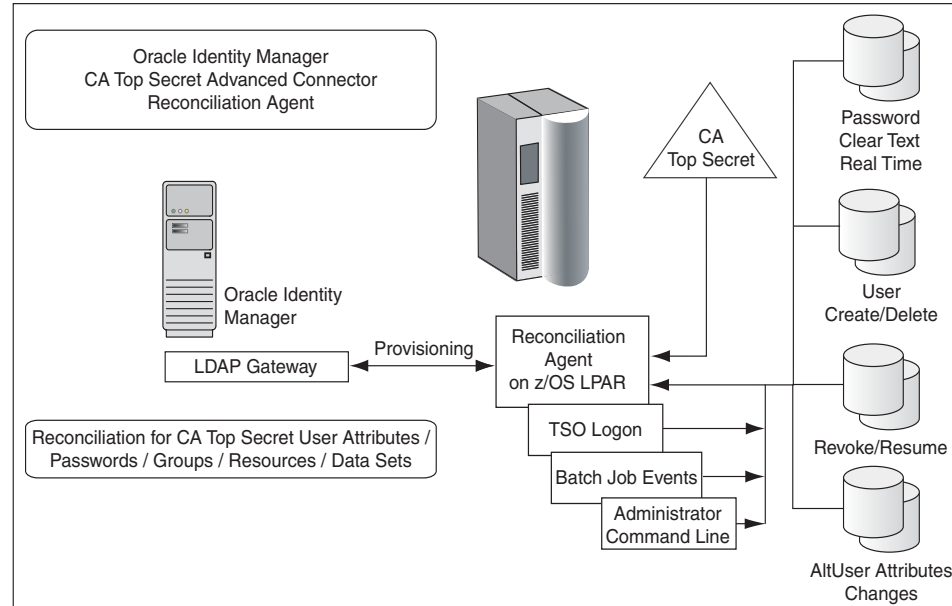
While not within the scope of standard Oracle Identity Management provisioning, the Provisioning Agent can extend control to TSO commands, CICS commands, batch jobs, and other mainframe resources.

Oracle Identity Manager Reconciliation Agent

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 Agent 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 Agent 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 Reconciliation Agent will notify Oracle Identity Manager and even create a corresponding account in Oracle Identity Manager.



Passwords fall into a special category. If business rules permit, a password change will be passed to 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 communication of connector resources and internal mainframe memory subpools for enterprise loads at peak times. The Reconciliation Agent 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 Oracle Identity Manager for subsequent processing (typically over the next hour). The entire Reconciliation Agent is protected by AES 128 encryption and APF authorized resources.

The Reconciliation Agent sends notification events to the Oracle Identity Manager LDAP Gateway from the z/OS mainframe. This architecture does not originate with CA Top Secret, 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

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

As with the Provisioning Agent, 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 Agent detected events from an LPAR exit, the Reconciliation Agent 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 Provisioning and Reconciliation Agent.

- 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 Agent. 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 Agent, not depending platform-specific programs or libraries.

The LDAP Gateway, Provisioning Agent, and Reconciliation Agent all coordinate bidirectional synchronization to a single 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 Agent and the other 10 are used for the Reconciliation Agent.

Messages between the LDAP Connector and the Provisioning Agent have a very short life span. The provisioning process that arises for 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 Agent require the same level of security and guaranteed delivery as MQ Series provides. Within this context, the Reconciliation Agent has been engineered for the following:

- If the TCP/IP connection has not been established between the Reconciliation Agent 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 Agent 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.

Index

A

Adapter Factory form, 2-6
Adapter Manager form, 2-6
adapters, compiling, 2-5
Administrative and User Console, 2-4
Advanced Encryption Standard, 1-2
APF Authorization, configuring, 3-9

C

CA Top Secret Advanced Connector
 architecture, B-1
 functionality, B-1
 LDAP Gateway, 1-1
 message transport layer, 1-1
 overview, 1-1
 Provisioning Agent, 1-1
 Reconciliation Agent, 1-1
changing input locale, 2-2
clustered environment, 2-6
compiling adapters, 2-5
configuring
 connector on a cluster, 2-6
 Oracle Identity Manager server, 2-2
connector
 deployment, 2-1
connector files and directories, 1-3
 copying, 2-2
 destination directories, 2-2
connector XML files
 See XML files
custom mainframe exits, 3-2

D

dataset resource profile attribute descriptions, A-3
defining
 IT resources, 2-4
deploying connector, 2-1
deployment
 connector agents, 3-2
 installing Reconciliation Agent exits, 3-3
 mainframe, 3-2
 Oracle Identity Manager system, 2-1
 requirements, verifying, 3-1

E

editing
 PIOCOPY, 3-6
 PIODEF, 3-7
 PIOMQ, 3-7
 PIONEER, 3-6
 VOYAGER, 3-8
 VOYCOPY, 3-8
 VOYDEF, 3-8
 VOYINIT, 3-8
 VOYKILL, 3-8
 VOYMQ, 3-8
 VOYSTOP, 3-8
exits
 installing, 3-3
 loading, 3-4
 permanent installation, 3-3
 uninstalling, 3-4
 viewing, 3-4

F

files and directories of the connector, 1-3
functionality supported, 1-2
functions available, 1-2

G

globalization features, 1-3
group attribute descriptions, A-2

I

IBM z/OS, 3-1
importing connector XML files, 2-4
initial program load, 3-2
initial reconciliation
 specific users, including and excluding, 4-2
 users, 4-1
input locale changing, 2-2
installation
 LDAP Gateway, 2-6
IPL*see* initial program load
issues, 6-1
IT resources
 defining, 2-4

parameters, 2-4
TopSecretResource IT Resource, 2-4

J

JAR files
copying, 2-2

L

LDAP Gateway, 1-1, 3-5, B-1
functionality, B-1
installing, 2-6
provisioning, configuration, 2-6
limitations, 6-1
logical partition, 3-2
LPARseellogical partition

M

mainframe
connector deployment, 3-2
deployment requirements, 3-1
environmental settings and requirements, 3-2
LPAR exits, 3-2
memory subpools, 3-2
mainframe repository, supported, 2-1
AES
See Advanced Encryption Standard
message transport layer, 1-1, 2-1
configuration, 3-4
configuring TCP/IP, 3-4
IP addresses, 3-5
MQ Series, 1-2, 2-1, 3-6
requirements, 2-2
TCP/IP, 2-1
TCP/IP with Advanced Encryption Standard, 1-2
using MQ Series, 3-4
MQ Series, 1-2, 2-1, 3-4
message transport layer, 3-6
PIOMQ, editing, 3-7
Provisioning Agent, installing, 3-6
Reconciliation Agent, dependency, 3-9
VOYMQ, editing, 3-8
multilanguage support, 1-3

N

node, configuring the connector on, 2-6

O

Oracle Identity Manager Administrative and User
Console, 2-4
Oracle Identity Manager server, configuring, 2-2

P

parameters of IT resources, 2-4
performance, tests, 5-4
PIOCOPY, editing, 3-6

PIODEF, editing, 3-7
PIOMQ, editing, 3-7
PIONEER, editing, 3-6
Provisioning Agent, 1-1, 1-2, 3-1, 3-5, B-1
functionality, 1-2, B-1
provisioning functions, 1-2
provisioning, configuration on LDAP Gateway, 2-6

R

reconciliation
configuring as a scheduled task, 4-2
trusted source, 4-2
Reconciliation Agent, 1-1, 1-2, 3-1, 3-5, B-1
dependency, MQ Series, 3-9
exits, installing, 3-3
functionality, 1-2, B-2
initial reconciliation run, 4-1
uninstalling exits, 3-4
reconciliation functions, 1-2

S

starter tasks, 3-10
building and operation, 3-10
supported
mainframe operating system, 3-1
mainframe repository, 2-1
Oracle Identity Manager versions, 2-1
target system host platform, 2-1
target systems, 2-1
supported languages, 1-3

T

target system host platforms, supported, 2-1
target systems, supported, 2-1
TCP/IP
configuring, 3-4
using as message transport layer, 3-4
TCP/IP with AES encryption, 2-1, 3-4
test cases, running, 5-2
testing
connectivity, 5-1
provisioning, 5-1
reconciliation, 5-1
troubleshooting, 5-3
trusted source reconciliation, 4-2

U

user attribute descriptions, A-1
user exit technology, 3-2

V

verifying deployment requirements, 3-1
VOYAGER, 3-7
VOYCOPY, 3-7
VOYDEF, 3-7
VOYINIT, 3-7

VOYKILL, 3-7
VOYMQ, 3-7
VOYSTOP, 3-8

X

XML files
 copying, 2-2
 importing, 2-4

