Oracle® Identity Manager

Connector Guide for CA Top Secret Advanced

Release 9.0.4

E10424-06

July 2009

Oracle Identity Manager Connector Guide for CA Top Secret Advanced, Release 9.0.4

E10424-06

Primary Author: Lyju Vadassery

Contributing Authors: Debapriya Datta, Devanshi Mohan, Alankrita Prakash

Contents

Preface

This guide provides information about integrating Oracle Identity Manager with CA Top Secret.

Audience

This guide is intended for resource administrators and target system integration teams.

Documentation Accessibility

Our goal is to make Oracle products, services, and supporting documentation accessible to all users, including users that are disabled. 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.

Deaf/Hard of Hearing Access to Oracle Support Services

To reach Oracle Support Services, use a telecommunications relay service (TRS) to call Oracle Support at 1.800.223.1711. An Oracle Support Services engineer will handle technical issues and provide customer support according to the Oracle service request process. Information about TRS is available at `http://www.fcc.gov/cgb/consumerfacts/trs.html`, and a list of phone numbers is available at `http://www.fcc.gov/cgb/dro/trsphonebk.html`.

Related Documents

For generic information about connectors, see *Oracle Identity Manager Connector Concepts*.

To access the Oracle Identity Manager documents mentioned as references in this guide, visit Oracle Technology Network. The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

`http://www.oracle.com/technology/documentation/index.html`

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connector Pack documentation library, visit Oracle Technology Network at

`http://www.oracle.com/technology/documentation/index.html`

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

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

This chapter provides an overview of the updates made to the software and documentation for the Oracle Identity Manager Connector for CA Top Secret in release 9.0.4.4.

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

- Software Updates

  This section describes updates made to the connector software.

- Documentation-Specific Updates

  This section describes major changes made to this guide. These changes are not related to software updates.

Software Updates

The following software updates have been made in this connector:

- Software Updates Up To Release 9.0.4.2
- Software Updates in Release 9.0.4.3
- Software Updates in Release 9.0.4.4

Software Updates Up To Release 9.0.4.2

The following are software updates up to release 9.0.4.2:

- The IBM MQ Series protocol for the message transport layer is no longer supported for this connector. All content related to this protocol has been removed from the guide.
- CA Top Secret user profile, group profile, facility, and data set and resource profile commands supported by the Provisioning Agent have been added in "Functionality Supported by the Pioneer Provisioning Agent" on page 1-6.
- The list of functions supported by the Provisioning Agent has been updated in "Functionality Supported for Provisioning" on page 1-7.
- The commands supported by the Reconciliation Agent have been added in "Functionality Supported by the Voyager Reconciliation Agent" on page 1-7.
- The list of functions supported by the Reconciliation Agent has been updated in "Functionality Supported for Reconciliation" on page 1-7.

- The list of fields reconciled between Oracle Identity Manager and CA Top Secret has been updated in "Target System Fields Used for Reconciliation and Provisioning" on page 1-8.
- The IT resource parameters and their corresponding descriptions and sample values have been updated in "Importing the Connector XML File" on page 2-6.
- The procedure to configure the connector for multiple installations of the target system has been added in "Configuring the Connector for Multiple Installations of the Target System" on page 2-13.
- Information about reconciliation based on user status has been added in "Configuring Account Status Reconciliation" on page 4-5.
- Steps to add a new field for provisioning have been added in "Adding New Fields for Provisioning" on page 4-6.
- Known issues related to the following bugs have been added in Chapter 6, "Known Issues":
  - 6668844
  - 6904041
  - 7033009
- Information about integrating the Reconciliation Agent exit with existing Top Secret exits has been added in "Installing the Reconciliation Agent Exit" on page 3-3.

Software Updates in Release 9.0.4.3

The following are resolved issues in release 9.0.4.3:

Bug Number	Issue	Resolution
7583557	Passwords were specified in unencrypted format in the `beans.xml` file, which is a configuration file used by the connector.	This issue has been resolved. You can now use the `propertyEncrypt` script to encrypt passwords before you copy them into the `beans.xml` file. See "Encrypting Passwords Used in the beans.xml File" for information about the procedure.

Software Updates in Release 9.0.4.4

The following are software updates in release 9.0.4.4:

- Support for Limited Reconciliation from Multiple Resources

Support for Limited Reconciliation from Multiple Resources

If you use multiple resource objects for reconciliation with the target system, then from this release onward you can specify the resource objects with which you want to associate records of specific user types from the target system. See "Configuring Limited Reconciliation" for more information about this feature.

Documentation-Specific Updates

The following documentation-specific updates have been made in releases 9.0.4.1 through 9.0.4.4:

- The user profile field mappings and resource profile field mappings between Oracle Identity Manager and the target system have been added in "Target System

Fields Used for Reconciliation and Provisioning" on page 1-8. Appendix A, "Attribute Mapping Between CA Top Secret and Oracle Identity Manager" has been removed.

- The components of the CA Top Secret Advanced connector and the connector architecture for reconciliation and provisioning have been added in "Connector Architecture" on page 1-3. Appendix B, "Connector Architecture" has been removed.
- Guidelines that were earlier documented in Chapter 6, "Known Issues" have been moved to "Guidelines on Using the Connector" on page 5-2.
- Information about enabling logging on the LDAP Gateway server has been added in "Installing and Configuring the LDAP Gateway" on page 2-8.
- In the "Functionality Supported for Reconciliation" section, the following functions have been added:
  - Suspend users until
  - UnSuspend uses until
- In the "User Field Mapping" section, the defaultGroup field has been removed.
- Some corrections have been made in the following sections:
  - Environmental Settings and Requirements
  - Deploying the Reconciliation Agent and Provisioning Agent
  - Installing the Reconciliation Agent Exit
  - Configuring TCP/IP Connection and Starter Tasks
- In the "Certified Languages" section, Arabic has been added to the list of languages that the connector supports.
- In Table 1–1, " Certified Deployment Configurations", changes have been made in the Target Systems row. Information about certified deployment configurations has been removed from "Verifying Deployment Requirements" on page 3-1.

1 About the Connector

The Oracle Identity Manager CA Top Secret Advanced connector provides a native interface between Oracle Identity Manager and CA Top Secret installed on a z/OS mainframe. The connector functions as a trusted virtual administrator on the target system, performing tasks, such as creating login IDs and changing passwords. In addition, it automates some of the functions that administrators usually perform manually.

This guide discusses the connector that enables you to use CA Top Secret either as a managed (target) resource or as an authoritative (trusted) source of user information for Oracle Identity Manager.

This chapter contains the following topics:

- Certified Deployment Configurations
- Certified Languages
- Features of the Connector
- Roadmap for Deploying and Using the Connector

1.1 Certified Deployment Configurations

Table 1–1 lists the certified deployment configurations.

Table 1–1 Certified Deployment Configurations

Item	Requirement
Oracle Identity Manager	Oracle Identity Manager release 8.5.3.1 or later
Target Systems	CA Top Secret r8 SP4 or later, r9 SP1or later, r12 SP2 or later
Message transport layer	TCP/IP with Advanced Encryption Standard (AES) encryption
Target system user account for Oracle Identity Manager	IBM Authorized Program Facility (APF) authorized account with SystemAdministrators privileges

> **Note:** The LDAP Gateway uses the target system user account that you create for Oracle Identity Manager. Therefore, it has the privileges required to access and operate with the Reconciliation Agent and Provisioning Agent. See "Connector Architecture" on page 1-3 for information about the Reconciliation Agent and Provisioning Agent.

1.1.1 Message Transport Layer Requirements

Between the Oracle Identity Manager and mainframe environments, Oracle Identity Manager uses the TCP/IP secure message transport layer.

Ports 5190 and 5790 are the default ports for the Reconciliation Agent and Provisioning Agent, respectively. You can change the ports for these agents.

1.1.2 Configuration of APF Authorization

Granting the APF-authorized status to a program is similar to granting superuser status. This process allows a program to run without allowing system administrators to query or interfere with its operation. The program that runs on the mainframe system and the user account it runs under must both have APF authorization. The Provisioning Agent user account must also have APF authorization.

> **Note:** APF authorization is usually granted by a mainframe administrator. If you do not have the required authority to perform such tasks, then enlist the assistance of someone who is qualified to perform these tasks.

1.2 Certified Languages

The connector supports the following languages:

- Arabic
- Chinese (Simplified)
- Chinese (Traditional)
- Danish
- English
- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazilian)
- Spanish

1.3 Features of the Connector

This section discusses the following topics:

- Connector Architecture
- Functionality Supported by the Pioneer Provisioning Agent
- Functionality Supported for Provisioning
- Functionality Supported by the Voyager Reconciliation Agent
- Functionality Supported for Reconciliation
- Target System Fields Used for Reconciliation and Provisioning

1.3.1 Connector Architecture

The connector consists of the following components:

- **LDAP Gateway:** The LDAP Gateway is built on Java 1.4 and allows portability across various platforms and operating systems. The LDAP Gateway receives LDAP protocol commands from distributed applications and translates them to native mainframe commands. After the commands are run, LDAP-formatted responses are returned to the requesting application. It is recommended that you install the LDAP Gateway on the same computer as Oracle Identity Manager.
- **Pioneer Provisioning Agent:** The connector provides the provisioning functionality through the Pioneer Provisioning Agent, which is a mainframe component. The Provisioning Agent receives native mainframe identity and authorization change events from the LDAP Gateway. These events are processed against the mainframe authentication repository, in which all provisioning updates from the LDAP Gateway are stored. The response is parsed and returned to the LDAP Gateway.
- **Voyager Reconciliation Agent:** The connector provides the reconciliation functionality through the Voyager Reconciliation Agent, which is a mainframe component. The Reconciliation Agent captures native mainframe events by using exit technology. Exits are programs that are run after a system event in the mainframe is processed. The Reconciliation Agent captures in real time events occurring from TSO logins, the command prompt, batch jobs, and other native mainframe events. The Reconciliation Agent transforms these events 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 Reconciliation Agent and Provisioning Agent. TCP/IP with AES encryption is the message transport layer that uses 128-bit cryptographic keys. The connector supports a message transport layer by using the TCP/IP protocol, which is functionally similar to proprietary message transport layer protocols.

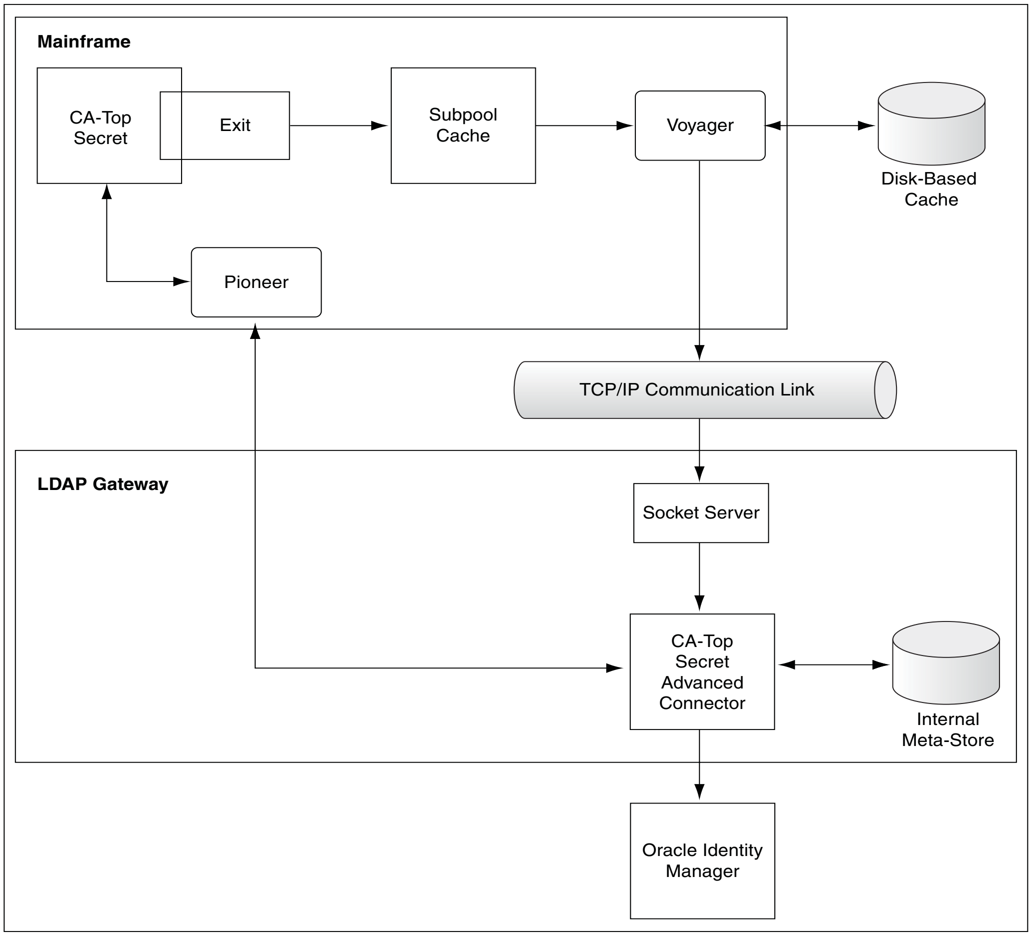
The architecture of the connector can be explained in terms of the operations it supports:

- Reconciliation
- Provisioning

1.3.1.1 Reconciliation

Figure 1–1 shows the flow of data during reconciliation.

Figure 1–1 Reconciliation Process



Reconciliation involves the following steps:

1. Mainframe identity and authorization events take place in the mainframe target system. These mainframe events are processed through appropriate exits.

> **Note:** Identity and authorization events in the mainframe system consist of Top-Secret ACID logon, running of a command, real-time password synchronization, creation or deletion of a user, or a change in the user attributes.

2. The mainframe events are stored in the subpool 231 cache of the Voyager Reconciliation Agent. Subpool 231 is an area of z/OS storage that the Reconciliation Agent uses to temporarily store CA Top Secret events. The subpool 231 cache enables the Reconciliation Agent to handle a large number of events from the mainframe.

3. The Reconciliation Agent reads these events, converts them from EBCDIC to ASCII, and then encrypts them using AES encryption. The Reconciliation Agent opens a new socket to the LDAP Gateway and sends the encrypted notification messages through the message transport layer. These messages contain the minimum amount of data required to reconcile the event, such as message type, user ID, and password (for a password change event).

Note: When the mainframe system is shut down, event records are stored offline. These offline events are reloaded in the Reconciliation Agent when the mainframe is started up.

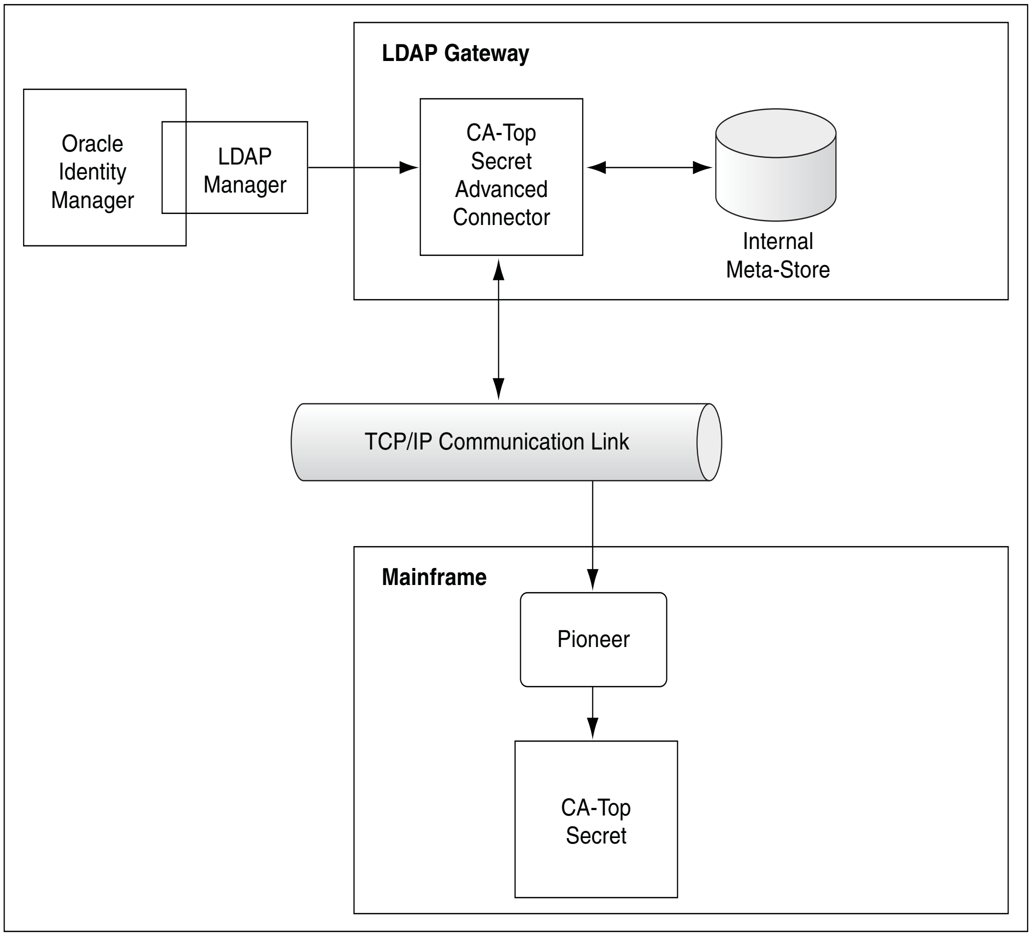
---

4. The LDAP Gateway receives the messages from the Reconciliation Agent and decrypts them for the connector.
5. The connector sends a request to the Provisioning Agent to retrieve all the current user data that is generated as a result of the mainframe identity and authorization events.
6. If an event fetched from the target system matches with the user data, then the connector returns an error and the process stops. If the event does not match, then the connector sends the event to Oracle Identity Manager for reconciliation processing and updates the internal meta-store of event records. This process is repeated for all the events that are fetched from the target system.

1.3.1.2 Provisioning

Figure 1–2 shows the flow of data during provisioning.

Figure 1–2 Provisioning Process



Provisioning involves the following steps:

1. A user is created, updated, or deleted in Oracle Identity Manager.

2. The Oracle Identity Manager process task adapter for CA Top Secret forwards the change request to the LDAP Gateway.
3. The LDAP Gateway translates the change request from the LDAP Gateway to mainframe commands. The CA Top Secret Advanced connector encrypts the data, and sends it to the Provisioning Agent through the message transport layer.
4. The connector also updates the internal meta-store of the LDAP Gateway with the changes in user data.
5. On the target system, the Provisioning Agent decrypts the data, sends the data to the mainframe repository, and returns the success or error messages back to the LDAP Gateway.

1.3.2 Functionality Supported by the Pioneer Provisioning Agent

The Pioneer Provisioning Agent supports the following functions:

- Standard CA Top Secret user profile commands:
  - [TSS CREATE]: Creates a CA Top Secret user profile
  - [TSS REPLACE]: Modifies an existing CA Top Secret user profile
  - [TSS DELETE]: Deletes a CA Top Secret user profile
- Standard CA Top Secret group profile commands:
  - [TSS ADDTO]: Adds a CA Top Secret user to a profile
  - [TSS REMOVE]: Removes a CA Top Secret user from a profile
- Standard CA Top Secret facility commands:
  - [TSS ADDTO]: Adds a CA Top Secret user to a facility
  - [TSS REMOVE]: Removes a CA Top Secret user from a facility
- Standard CA Top Secret data set and resource profile commands:
  - [TSS PERMIT]: Provides data set or resource profile access to a user

1.3.3 Functionality Supported for Provisioning

Table 1–2 describes the functions supported by the Provisioning Agent.

Table 1–2 Functionality Supported for Provisioning

Function	Description
Create Users	Adds new users in CA Top Secret.
Modify Users	Modifies user information in CA Top Secret.
Change Passwords	Changes user passwords on CA Top Secret in response to password changes made on Oracle Identity Manager through user self-service.
Reset Passwords	Resets user passwords on CA Top Secret. The passwords are reset by the administrator.
Suspend User Accounts	Disables user accounts. in CA Top Secret
Unsuspend User Accounts	Enables user accounts in CA Top Secret.
Delete Users	Removes user accounts from CA Top Secret.
Grant User Access To Data Sets	Adds user to data set with access rights.

Table 1–2 (Cont.) Functionality Supported for Provisioning

Function	Description
Grant User Access To Privileges (TSO)	Provides TSO login access to the user.

1.3.4 Functionality Supported by the Voyager Reconciliation Agent

The Voyager Reconciliation Agent supports reconciliation of changes that are made to user profiles by using commands such as ADDUSER or ALTUSER. These commands may also contain users' passwords for reconciliation, if any.

1.3.5 Functionality Supported for Reconciliation

The Reconciliation Agent supports the following functions:

- Change passwords
- Password resets
- Create user data
- Modify user data
- Suspend users
- Suspend users until
- Delete users
- Unsuspend users
- UnSuspend uses until

1.3.6 Target System Fields Used for Reconciliation and Provisioning

This section discusses the following topics:

- User Field Mapping
- Profile Field Mapping

1.3.6.1 User Field Mapping

Table 1–3 lists the user fields that are reconciled between Oracle Identity Manager and the target system.

Table 1–3 Field Mapping Between Oracle Identity Manager and CA Top Secret

Oracle Identity Manager Field	CA Top Secret Field	Description
uid	USER	Login ID of the user
cn	NAME	Full name of the user
sn	NAME	Last name of the user
givenName	NAME	First name of the user
userPassword	PASSWORD	Password
attributes	SPECIAL, AUDITOR, GPRACC, OPERATIONS	Attributes of the user
department	DEPARTMENT	Default department of the user

Table 1–3 (Cont.) Field Mapping Between Oracle Identity Manager and CA Top Secret

Oracle Identity Manager Field	CA Top Secret Field	Description
instdata	DATA	Installation-defined data of the user
createdate	CREATED	Date user was created
passwordExpireDate	EXPIRES	Date the user's password expires
passwordExpireInterval	INTERVAL	Number of days the user's password remains valid
suspendUntilDate	SUSPENDED DATE	Future date on which the user will be prevented from accessing the system
memberOf	PROFILE	Profile information for the user
facilities	FACILITY	Facility information for the user
division	DIVISION	Default division for the user
lastmodificationdate	LAST MOD	Last time the user connected
tsocommand	COMMAND	Command to be run during TSO/E logon
tsodest	DEST	Default SYSOUT destination
tsounit	UNIT	Default unit name for allocations
tsoudata	USERDATA	Site-defined data field for a TSO user
tsoalcct	ACCTNUM	Default TSO account number on the TSO/E logon panel
tsohclass	HOLDCLASS	Default hold class
tsojclass	JOBCLASS	Default job class
tsomaxsize	MAXSIZE	Maximum region size the user can request at logon
tsomclass	MSGCLASS	Default message class
tsolproc	PROC	Default logon procedure on the TSO/E logon panel
tsolsize	SIZE	Minimum region size if not requested at logon
tsolopt	OPT	TSO options, such as MAIL and NOTICES
tsosclass	SYSOUTCLASS	Default SYSOUT class
revoke	NA	Value 'Y' if user is revoked or 'N' if user is not revoked

1.3.6.2 Profile Field Mapping

Table 1–4 lists the profile field mappings between Oracle Identity Manager and the target system.

Table 1–4 Profile Field Descriptions

Oracle Identity Manager Field	CA Top Secret Field	Description
cn	PROFILE	Profile ID
uniqueMember	USERS	Users associated with the profile

1.4 Roadmap for Deploying and Using the Connector

Deploying the connector involves deploying the LDAP Gateway, Reconciliation Agent, and Provisioning Agent. The Reconciliation Agent and Provisioning Agent are deployed on the mainframe.

These procedures are described in the following chapters:

- Chapter 2, "Connector Deployment on Oracle Identity Manager" provides instructions for deploying the connector on the Oracle Identity Manager system. This procedure involves configuring Oracle Identity Manager, importing the connector XML file, compiling adapters, installing the LDAP Gateway, and configuring the message transport layer.
- Chapter 3, "Connector Deployment on CA Top Secret" describes the procedure to deploy the Reconciliation Agent and Provisioning Agent on the mainframe. It is recommended that you perform this procedure with the assistance of the systems programmer.
- Chapter 4, "Configuring the Connector" describes the procedure to run initial reconciliation and to configure trusted source reconciliation and account status reconciliation.
- Chapter 5, "Troubleshooting" discusses the problems that you might encounter while using the connector. In addition, this chapter discusses guidelines on using the connector.
- Chapter 6, "Known Issues" lists known issues associated with this release of the connector.

2

Connector Deployment on Oracle Identity Manager

The following sections describe the procedure to deploy the LDAP Gateway on the Oracle Identity Manager host computer:

- Files and Directories That Comprise the Connector
- Copying the Connector Files
- Configuring Oracle Identity Manager
- Importing the Connector XML File
- Compiling Adapters
- Installing and Configuring the LDAP Gateway

Refer to the following section if you want to configure the connector for multiple installations of the target system:

- Configuring the Connector for Multiple Installations of the Target System

> **See Also:** Chapter 3, "Connector Deployment on CA Top Secret" for the procedure to deploy the Reconciliation Agent and Provisioning Agent on the mainframe

2.1 Files and Directories That Comprise the Connector

Table 2–1 describes the contents of the connector installation media.

Table 2–1 Files and Directories That Comprise the Connector

Files and Directories	Description of Files and Contents
etc/LDAP Gateway/ldapgateway.zip	Files required to deploy the LDAP Gateway.
Files in the etc/Provisioning and Reconciliation Connector/ directory	Files required to deploy the Provisioning Agent and the Reconciliation Agent on the mainframe.
lib/idm.jar	Connector JAR file to be deployed on the Oracle Identity Manager system. It contains the Oracle Identity Manager process tasks adapter code.
lib/topsecret-adv-agent-recon.jar lib/topsecretConnection.properties	Files required for real-time reconciliation between the target system and Oracle Identity Manager.

Table 2–1 (Cont.) Files and Directories That Comprise the Connector

Files and Directories	Description of Files and Contents
Files in the resources directory	Each of these resource bundles contains locale-specific information that is used by the connector. **Note:** A **resource bundle** is a file containing localized versions of the text strings that are displayed on the user interface of Oracle Identity Manager. These text strings include GUI element labels and messages displayed on the Administrative and User Console.
Files in the scripts directory: - run_initial_recon_provisioning.sh - run_initial_recon_provisioning.bat - initialTopSecretAdv.properties - topsecret-adv-initial-recon.jar	Files that are used to perform first-time (initial) reconciliation with Oracle Identity Manager.
scripts/user.txt	Sample of the file containing user data that is used during initial reconciliation. This file is discussed in detail in "Running Initial Reconciliation" on page 4-3.
xml/oimTopSecretAdvancedConnector.xml	This XML file contains definitions for the connector components related to reconciliation and provisioning. These components include: - Resource objects - IT resource types - Process forms - Process tasks and adapters - Provisioning process - Lookup definitions - Prepopulate rules - Scheduled tasks
xml/oimTopSecretTrustedXellerateUser.xml	The XML file that contains component definitions for the connector for trusted source reconciliation.

2.2 Copying the Connector Files

Copy the connector files to the destinations on the Oracle Identity Manager host computer as indicated in Table 2–2.

Note: See "Files and Directories That Comprise the Connector" on page 2-1 for more information about these files. Do not copy the files that are not listed in this table. Those files are used later in the deployment procedure.

Table 2–2 Copying the Connector Files

Files	Destination
etc/LDAP Gateway/ldapgateway.zip	*LDAP_INSTALL_DIR* This is the directory on the Oracle Identity Manager host computer where you want to install the LDAP Gateway. See "Installing and Configuring the LDAP Gateway" on page 2-8 for information about installing the LDAP Gateway.
lib/topsecret-adv-agent-recon.jar lib/topsecretConnection.properties	*LDAP_INSTALL_DIR*/etc
lib/idm.jar Files in the scripts directory: ■ run_initial_recon_provisioning.sh ■ run_initial_recon_provisioning.bat ■ topsecret-adv-initial-recon.jar ■ user.txt ■ initialTopSecretAdv.properties	`OIM_HOME/xellerate/JavaTasks/`
Files in the resources directory	`OIM_HOME/xellerate/connectorResources/`
xml/oimTopSecretAdvancedConnector.xml xml/oimTopSecretTrustedXellerateUser.xml	`OIM_HOME/xellerate/XLIntegrations/tops/xml/`

Note: While installing Oracle Identity Manager in a clustered environment, you copy the contents of the installation directory to each node of the cluster. Similarly, you must copy the files in the connectorResources directory and the JAR files to the corresponding directories on each node of the cluster.

2.3 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

- Clearing Content Related to Connector Resource Bundles from the Server Cache
- Enabling Logging

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

2.3.1 Clearing Content Related to Connector Resource Bundles from the Server Cache

When you perform the procedure described in "Copying the Connector Files" on page 2-2, you copy the resource bundles for this connector into the OIM_HOME/xellerate/connectorResources directory. Whenever you add a new resource bundle in the connectorResources directory or make a change in an existing resource bundle, you must clear content related to connector resource bundles from the server cache.

To clear content related to connector resource bundles from the server cache:

1. In a command window, go to the *OIM_HOME*/xellerate/bin/ directory.

> **Note:** You must perform step 1 before you perform step 2. An exception is thrown if you run the command described in Step 2 as follows:
>
> ```
> OIM_HOME/xellerate/bin/BATCH_FILE _NAME
> ```

2. Enter one of the following commands:

   - On Microsoft Windows:

     ```
     PurgeCache.bat ConnectorResourceBundle
     ```

   - On UNIX:

     ```
     PurgeCache.sh ConnectorResourceBundle
     ```

   > **Note:** You can ignore the exception that is thrown when you perform Step 2. This exception is different from the one mentioned in Step 1.

   In this command, ConnectorResourceBundle is one of the content categories that you can remove from the server cache. Refer to the following file for information about the other content categories:

   ```
   OIM_HOME/xellerate/config/xlConfig.xml
   ```

2.3.2 Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. To specify the type of event for which you want logging to take place, you can set the log level to one of the following:

- ALL

  This level enables logging for all events.

- DEBUG

  This level enables logging of information about fine-grained events that are useful for debugging.

- INFO

  This level enables logging of messages that highlight the progress of the application at a coarse-grained level.

- WARN

  This level enables logging of information about potentially harmful situations.

- ERROR

  This level enables logging of information about error events that might allow the application to continue running.

- FATAL

  This level enables logging of information about very severe error events that could cause the application to stop functioning.

- OFF

  This level disables logging for all events.

The file in which you set the log level and the log file path depend on the application server that you use:

- **JBoss Application Server**

  To enable logging:

  1. In the *JBOSS_HOME*/server/default/conf/log4j.xml file, add the following lines:

     ```
     <category name="IdfTopsUserOperations">
        <priority value="LOG_LEVEL"/>
     </category>
     ```

  2. In the second XML line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     ```
     <category name="IdfTopsUserOperations">
        <priority value="INFO"/>
     </category>
     ```

  After you enable logging, log information is written to the following file:

  `JBOSS_HOME/server/default/log/server.log`

- **IBM WebSphere Application Server:**

  To enable logging:

  1. In the *OIM_HOME*/xellerate/config/log.properties file, add the following line:

     ```
     log4j.logger.IdfTopsUserOperations=LOG_LEVEL
     ```

  2. In this line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     ```
     log4j.logger.IdfTopsUserOperations=INFO
     ```

  After you enable logging, log information is written to the following file:

  `WEBSPHERE_HOME/AppServer/logs/SERVER_NAME/SystemOut.log`

- **BEA WebLogic Server**

  To enable logging:

  1. In the *OIM_HOME*/xellerate/config/log.properties file, add the following line:

     ```
     log4j.logger.IdfTopsUserOperations=LOG_LEVEL
     ```

  2. In this line, replace *LOG_LEVEL* with the log level that you want to set. For example:

     ```
     log4j.logger.IdfTopsUserOperations=INFO
     ```

  After you enable logging, log information is displayed on the server console.

- **Oracle Application Server**

  To enable logging:

1. In the *OIM_HOME*/xellerate/config/log.properties file, add the following line:

   ```
   log4j.logger.IdfTopsUserOperations=LOG_LEVEL
   ```

2. In this line, replace *LOG_LEVEL* with the log level that you want to set. For example:

   ```
   log4j.logger.IdfTopsUserOperations=INFO
   ```

After you enable logging, log information is written to the following file:

```
OAS_HOME/opmn/logs/default_group~home~default_group~1.log
```

2.4 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 oimTopSecretAdvancedConnector.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 IT resource is displayed.
8. Specify values for the parameters of the OIMTopSecretResourceObject IT resource. Table 2–3 lists the values to be specified.

Table 2–3 Defining IT Resources

Parameter	Description
AtMap User	Name of the lookup definition containing attribute mappings that are used for provisioning Value: `AtMap.TopSecret` **Note:** You must not change the value of this parameter.
idfPrincipalDn	Administrator ID for connecting to the LDAP Gateway Sample value: `cn=idfTopsAdmin,dc=tops,dc=com`
idfPrincipalPwd	Administrator password for connecting to the LDAP Gateway

Table 2–3 (Cont.) Defining IT Resources

Parameter	Description
idfRootContext	Root context for CA Top Secret Value: `dc=tops,dc=com` **Note:** You must not change the value of this parameter.
idfServerHost	Host name for connecting to the LDAP Gateway Value: `localhost` **Note:** You must not change the value of this parameter.
idfServerPort	Port for connecting to the LDAP Gateway Sample value: `5389`

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.
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. These nodes represent Oracle Identity Manager entities that are redundant. Before you import the connector XML file, you must remove these entities by right-clicking each node and then selecting **Remove**.
12. Click **Import**. The connector file is imported into Oracle Identity Manager.

2.5 Compiling Adapters

Adapters are used to implement provisioning functions. The following adapters are imported into Oracle Identity Manager when you import the connector XML file:

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

- ResumeTopsUserUntil

You must compile these adapters before they can be used in provisioning operations. 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, click **Compile All**.

   If you have created your own adapters or if a new adapter is shipped with a patch that you installed, then you might need to compile one adapter at a time. To compile multiple (but not all) adapters, select the adapters you want to compile. Then, click **Compile Selected**.
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.

2.6 Installing and Configuring the LDAP Gateway

To install and configure the LDAP Gateway:

1. Extract the contents of the ldapgateway.zip file to a directory on the computer on which Oracle Identity Manager is installed.

   Note: In this document, the location (and name) of the ldapgateway directory is referred to as *LDAP_INSTALL_DIR*.

2. In a text editor, open the following scripts:
   - Open the run.sh or run.bat script from the *LDAP_INSTALL_DIR*/bin/ directory.
   - Open the run_initial_recon_provisioning script from the *OIM_HOME*/Xellerate/JavaTasks directory.
3. In the run script:
   - Set the JAVA_HOME property as follows:

     ```
     JAVA_HOME=DIRECTORY_LOCATION\j2sdj1.4.2_13
     ```

     Replace *`DIRECTORY_LOCATION`* with the full path of the directory.
   - If you plan to run multiple LDAP Gateways on a Linux or Solaris environment and there are not enough socket file descriptors to open up all the ports needed for the server, then add the following line:

     ```
     -Djava.nio.channels.spi.SelectorProvider=sun.nio.ch.PollSelectorProvider
     ```

4. In the run and run_initial_recon_provisioning scripts, uncomment the line related to the application server directory. In addition, change the path to reflect the actual location of the application server directory.

   Note: The contents of the run and run_initial_recon_provisioning scripts are similar. You must make the same change in both the scripts.

The lines starting with a number sign (#) are comments, as shown:

```
##### SET JBOSS HOME ##################
#APPSERVER_HOME=/opt/ldapgateway/lib/jboss-4.0.2
```

To uncomment the line, remove the number sign. For example, to ensure that the connector works with JBoss Application Server, change the line to the following:

```
##### SET JBOSS HOME ##################
APPSERVER_HOME=/opt/ldapgateway/lib/jboss-4.0.2
```

5. If you are using IBM WebSphere Application Server 6.1, then add the com.ibm.ws.wccm_6.1.0.jar file to the CLASSPATH variable in the run and run_initial_recon_provisioning scripts as shown in the following example:

```
rem
rem SET WEBSPHERE APPLICATION SERVER REQUIRED LIBRARIES
rem
set CLASSPATH=%CLASSPATH%;"%APPSERVER_HOME%"\lib\com.ibm.ws.wccm_6.1.0.jar
```

6. In a text editor, open the *LDAP_INSTALL_DIR*/conf/TOPS.properties file. In this file, specify information for the following properties of the message transport layer that you use:

For TCP/IP, the default values are as follows:

```
_type_=socket
_isencrypted_=true
_timeout_=5000
_authretries_=2
_host_=HOST_NAME_OR_IP_ADDRESS_OF_MAINFRAME
_port_=5790
_agentport_=5190
_nameFormat_=fn|sp|ln
_configSegment_=METADIR
_configAttrs_=ATTR1|ATTR2
```

The configurable properties are:

– _type_: The transport type, which is TCP/IP (socket).

– _host_: The host name or IP address of the mainframe.

Note: If you are configuring the LDAP Gateway on the computer on which Oracle Identity Manager is installed, then specify `localhost` as the value of the _host_ property. If you are configuring the LDAP Gateway on a different computer, then specify the host name or IP address of the computer as the value of the _host_ property. However, it is recommended that you install the LDAP Gateway on the same computer on which Oracle Identity Manager is installed.

– _port_: The port of the Pioneer Provisioning Agent.

– _agentport_: The port that the Reconciliation Agent uses to send messages.

– _nameFormat_: The property used to specify the format of the Full Name attribute.

– _configSegment_: The property used to specify the name of the segment. A segment indicates how profile information is segregated in CA Top Secret.

METADIR is an example of a segment. Examples of default segments are PASSWORD and CICS.

- _configAttrs_: For reconciliation, you add the custom fields to the _configAttrs_ property in the TOPS.properties file that match the name of the CA Top Secret field.

7. In the TOPS.properties file, use the following property to specify whether you want to revoke access rights or delete users during Disable User provisioning operations:

```
# DEFAULT ACTION WHEN DELETE FUNCTION USED
_defaultDelete_=delete
```

Set `revoke` as the value of this property if you want the user to be disabled on the target system as the outcome of a Delete User provisioning operation.

Set `delete` as the value of this property if you want the user to be deleted from the target system as the outcome of a Delete User provisioning operation.

8. In the TOPS.properties file, use the _nameFormat_ property to specify the format of the Full Name attribute.

You can use the following as the components of the format that you specify:

- Use fn to represent the first name.
- Use sp to represent the space character.
- Use ln to represent the last name.
- Use a comma (,) to represent the comma.
- Use a period (.) to represent the period.
- Use the vertical bar (|) as the separator for the other components.

The following line shows a sample value for the _nameFormat_ property:

```
_nameFormat_=fn|sp|ln
```

9. Open the *LDAP_INSTALL_DIR*/etc/topsecretConnection.properties file and edit the following property:

Note: You must also make this change in the initialTopSecretAdv.properties file, which is in the *OIM_HOME*/xellerate/JavaTasks directory.

```
_itResource_=NAME_OF_THE_NEW_IT_RESOURCE
```

Replace *NAME_OF_THE_NEW_IT_RESOURCE* with the name of the IT resource that you create by performing Step 8 of the procedure described in "Importing the Connector XML File" on page 2-6.

10. From the *LDAP_INSTALL_DIR*/dist/idfserver.jar file, extract the beans.xml file, open it in an editor, and set values for the following:

- Target system administrator credentials

  You must change the administrator credentials stored in the following lines of the beans.xml file:

Note: In these lines, the values that you can change are highlighted in bold font. The values that you enter in the beans.xml file must be the same as the values that you specify for the IT resource parameters and the properties in the topsecretConnection.properties and initialTopSecretAdv.properties files.

See "Encrypting Passwords Used in the beans.xml File" for information about encrypting the password before you enter it in the beans.xml file.

```
<property name="adminUserDN" value="cn=oimTOPSAdmin,dc=TOPS,dc=com"/>
<property name="adminUserPassword" value="password"/>
```

- Port used for communication between the LDAP Gateway and the mainframe logical partition (LPAR) that you use for the connector installation

  The default value of the port property is `5389`. If you want to change this value, then edit the value of the `port` property defined in the `beans.xml` file:

  ```
  <property name="port" value="5389"/>
  ```

11. To enable logging on the LDAP Gateway server:

    a. Extract the log4j.properties file from the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.

    b. Ensure that the log4j.rootLogger variable is set to the following:

    ```
    log4j.rootLogger=DEBUG, A1
    ```

    c. Save and close the file.

    When you use the connector, the following LDAP Gateway log files are generated in the *LDAP_INSTALL_DIR*/logs directory:

    - idfserver.log.0: This is the main log file.
    - topsecret-agent-recon.log: This is ongoing reconciliation log file that stores Oracle Identity Manager reconciliation messages.
    - topsagent.log.0: This file is currently redundant, and it will be removed in a later release.

12. Save the changes made to the beans.xml file, and then re-create the idfserver.jar file.

Note:

- When you start using the connector, the logs for the LDAP Gateway are created in the *LDAP_INSTALL_DIR*/logs directory.
- After editing the run.bat or run.sh file, you can start and stop the LDAP Gateway by running the following commands:

  To start LDAP Gateway on UNIX, run:

  ```
  bin> ./run.sh
  ```

  To stop LDAP Gateway on UNIX, run:

  ```
  bin> ./stop.sh
  ```

  To start LDAP Gateway on Microsoft Windows, run:

  ```
  bin>run.bat
  ```

  To stop LDAP Gateway on Microsoft Windows, enter `Ctrl + C` in the command window.

Encrypting Passwords Used in the beans.xml File

To encrypt passwords that you want to enter in the `beans.xml` file:

1. In a text editor, copy one of the following script files from the installation media into a temporary directory and then open the script file in a text editor:

   For Microsoft Windows:

   ```
   /scripts/propertyEncrypt.bat
   ```

   For UNIX:

   ```
   /scripts/propertyEncrypt.sh
   ```

2. Specify values for the following properties in the file:

   ```
   SET CLASSPATH=DIRECTORY_LOCATION\idfserver.jar
   ```

   Replace *DIRECTORY_LOCATION* with the full path of the directory into which you copied the idfserver.jar file while deploying the connector.

   For example:

   ```
   SET CLASSPATH=C:\software\identityforge\ldapgateway\dist\idfserver.jar
   ```

   ```
   %JAVACMD%  %JVM_OPTS%  -cp %CLASSPATH%
   com.identityforge.idfserver.util.AESCipherUtil PLAINTEXT_PASSWORD
   ```

   Replace *PLAINTEXT_PASSWORD* with the password that you want to encrypt.

   For example:

   ```
   %JAVACMD%  %JVM_OPTS%  -cp %CLASSPATH%
   com.identityforge.idfserver.util.AESCipherUtil idfTopsPwd
   ```

3. Save the changes made to the `propertyEncrypt.bat` or `propertyEncrypt.sh` script file.
4. Run the script.

The script encrypts the password that you provide and displays it in the command window.

5. Copy the encrypted password into the `beans.xml` file as follows:

   a. Extract the beans.xml file from the *`LDAP_INSTALL_DIR`*`/dist/idfserver.jar` file.

   b. In this file, search for the following string:

      ```
      <property name="adminUserPassword"
      ```

   c. Replace the value of this property with the encrypted password.

      For example:

      ```
      <property name="adminUserPassword"
      value="468018DD1CDBE82E515EBF78A41C428E"/>
      ```

2.7 Configuring the Connector for Multiple Installations of the Target System

You can configure the connector for multiple installations of the target system. You can also configure the connector for a scenario in which multiple logical partitions (LPARs), which are not associated with the first LPAR, are configured in the target system.

For each installation of the target system, you create an IT resource and configure an additional instance of the LDAP Gateway.

To configure the connector for the second installation of the target system:

> **Note:** Perform the same procedure for each installation of the target system.

1. Create an IT resource based on the OIMLDAPGatewayResourceType IT resource type.

   See Also:

   - *Oracle Identity Manager Design Console Guide* for information about creating IT resources
   - Step 8 of "Importing the Connector XML File" on page 2-6 for information about the parameters of the IT resource

2. Copy the current *`LDAP_INSTALL_DIR`* directory, including all the subdirectories, to a new location.

   > **Note:** In the remaining steps of this procedure, *LDAP_INSTALL_DIR* refers to the newly copied directory.

3. Extract the contents of the *LDAP_INSTALL_DIR*/dist/idfserver.jar file.

4. In the beans.xml file, change the value of the port in the <property name="port" value="xxxx"/> line to specify a port that is different from the port used for the

first instance of the LDAP Gateway. The default port number is shown in the following example:

```
<bean id="listener" class="com.identityforge.idfserver.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>
```

If you change the port number, then you must make the same change in the value of the `idfServerPort` parameter of the IT resource that you create.

5. Save and close the beans.xml file.
6. Open the *LDAP_INSTALL_DIR*/conf/TOPS.properties file and edit the following parameters:
   - _host_=*IP_ADDRESS_OR_HOST_NAME_OF_THE_MAINFRAME*
   - _port_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_PROVISIONING_AGENT*
   - _agentPort_=*PORT_OF_THE_SECOND_INSTANCE_OF_THE_RECONCILIATION_AGENT*

   > **Note:** The value of the _agentPort_ parameter must not be the same as that of the first instance if a second LPAR, which is not associated with the first LPAR, is configured in the target system. This value can be the same as the value of the idfServerPort parameter if you have two mainframe servers with CA Top Secret running on each server.

7. Open the *LDAP_INSTALL_DIR*/etc/TopSecretConnection.properties file and edit the following property:

   itResource=*NAME_OF_THE_NEW_IT_RESOURCE*

3 Connector Deployment on CA Top Secret

You must install the Reconciliation Agent and Provisioning Agent components of the CA Top Secret Advanced connector on the mainframe. The following sections describe the installation and configuration of these agents:

- Verifying Deployment Requirements
- Deploying the Reconciliation Agent and Provisioning Agent
- Installing the Reconciliation Agent Exit
- Configuring TCP/IP Connection and Starter Tasks

3.1 Verifying Deployment Requirements

Both the Reconciliation Agent and Provisioning Agent need a started task and service account that has the privileges required to run CA Top Secret system commands on the mainframe system.

In addition, both the Reconciliation Agent and Provisioning Agent require a surrogate Top-Secret ACID. This ACID must have administrative privileges to issue creates, changes, lists, and replaces.

> **Note:** Both the Reconciliation Agent and Provisioning Agent require executable code (z/OS loadlibs) to be APF authorized. This can be achieved by a dynamic set command (T PROG=) or by placing the installation loadlib containing the executable code in the z/OS Linklist.

3.1.1 Environmental Settings and Requirements

Ensure that the following requirements are met on the mainframe:

- The Provisioning Agent and Reconciliation agent use created z/OS subpool to manage peak load conditions. The subpool (231), which is allocated below the 16M line, requires 200 KB of memory for storage of Top-Secret events.
- The Reconciliation Agent operates by using exit technology, within the z/OS operating system environment.

  Command execution is captured by an exit, just before full completion of the native mainframe command. If the exit fails, then the command fails and returns an error message. Maintaining a specific password format is an example of the objective for which you use custom exits. Oracle Identity Manager exits are engineered to be the last exits called in sequence, which allows the existing exits to function normally. After modifying exits within an LPAR, an initial program load (IPL) of the LPAR may be required.

Note: The systems programmer must perform an IPL after a system component is changed or modified.

3.2 Deploying the Reconciliation Agent and Provisioning Agent

To deploy the Reconciliation Agent and Provisioning Agent:

1. Extract the contents of the following file from the installation media to a temporary directory on any computer:

   ```
   etc/Provisioning and Reconciliation Connector/Mainframe_TS.zip
   ```

2. The following JES2 xmit files are included in the TSS-Adapter package:
   - Linklib.xmi: Executable library for all modules
   - parmlib.xmi: PROG member for dynamically authorizing IDF.LINKLIB
   - prclib.xmi: Contains all the STC (Started Task Procedures)
   - maclib.xmi: z/OS maclib containing TSSINSTX source code
3. Log in to the TSO environment of the mainframe.
4. Perform the following steps either from the TSO 'Ready' prompt or by using ISPF Option #6 using a TN3270 or TN3270E emulator (each file must be uploaded without any file conversion and in binary):

   Note: You can also use FTP to upload the files.

   a. Upload each file to z/OS.

   b. Run the 'Receive inda(file-name-uploaded)' command for each file uploaded.

   c. When prompted for dataset names, use the following information:

   linklib.xmi: IDF.LINKLIB

   parmlib.xmi: IDF.PARMLIB

   prclib.xmi: IDF.PROCLIB

   maclib.xmi: IDF.MACLIB
5. To complete the installation, add 'IDF.LINKLIB' to the Linklist member of SYS1.PARMLIB or the installation parmlib used for the z/OS IPL.
6. Pioneer and Voyager require a Top-Secret ACID for operation and a set of permissions. The following is an example of the steps to be performed:

   Note: In these sample steps, xxxxxx is the ACID. This ID must be an administrator ID and with the permissions required to perform operations such as Create, Add, Addto, Replaces, and Changes. The following definitions are only an example in a test type environment.

   Create(xxxxxx) type(sca) name('pionvgr') password(nopw) facility(batch,stc)

```
Add(xxxxxx) uid(0) group(omvsgrp) dfltgrp(omvsgrp) home(/) omvspgm(/bin/sh)
Addto(stc) procname(pioneer) acid(xxxxxx)
Addto(stc) procname(voyager) acid(xxxxxx)
permit(xxxxxx) ibmfac(bpx.*) access(read)
permit(xxxxxx) ibmfac(irr.radmin.*) access(read)
add(xxxxxx) fac(all)
admin(xxxxxx) resource(all)
admin(xxxxxx) data(all)
admin(xxxxxx) acid(all)
admin(xxxxxx) facility(all)
admin(xxxxxx) misc1(all)
admin(xxxxxx) misc2(all)
admin(xxxxxx) misc3(all)
admin(xxxxxx) misc4(all)
admin(xxxxxx) misc8(all)
admin(xxxxxx) misc9(all)
```

3.3 Installing the Reconciliation Agent Exit

Because the exit modules are in the z/OS Load Library, an IPL may or may not be required to complete the installation. This depends on whether the z/OS Load Library is added to the LinkList, which is a z/OS storage area defined when an IPL is performed. To allow the LDAP Gateway to fully capture events, the Reconciliation Agent and its exits must be installed on each LPAR that shares the authentication repository.

The following are guidelines regarding the Reconciliation Agent exit:

- The Reconciliation Agent is installed in a z/OS Load Library for execution.
- The exit (TSSINSTX) must be accessible by the operating system after the IPL is started.
- It can be in the Linklist or steplib'ed to the STC (Reconciliation Agent).
- The Reconciliation Agent exit must be active and the subpool that contains TSS events must be active. If the exit is not active or subpool not activated (by executing Startup), then Top Secret events are not captured and sent to the LDAP gateway.
- In a single-LPAR environment, the Reconciliation Agent is required for real-time reconciliation event capture and the Provisioning Agent is required for provisioning.
- In a multiple-LPAR environment where the Top Secret database is shared, a master LPAR runs the Reconciliation Agent and Provisioning Agent. In addition, TSSINSTX must be installed and the subpool must be active.
- All Top Secret events from other LPARs are sent through the CPF to the master.

- If the CPF is not installed, then events are not captured and the Reconciliation Agent and Provisioning Agent are required on each LPAR.

This section also discusses the following topics:

- Installing the Reconciliation Agent Exit
- Integrating Exits

3.3.1 Installing the Reconciliation Agent Exit

Note: If there are no other exits installed on Top Secret, then perform the procedure described in this section.

To install the Reconciliation Agent exit:

1. Copy the exit from IDF.LINKLIB to a user-defined CA loadlib, which is in the Linklist for the LPAR.
2. Add the user-defined CA Loadlib to the SYS1.PARMLIB member PROG=.
3. Perform an IPL on z/OS.
4. Run the following command from the z/OS operator's console to activate the exit code:

   ```
   'F TSS,EXIT(ON')
   ```

Note: There is only one exit within a CA Top Secret environment. Typically, a production deployment has its own custom changes already written into the exit. The exit supplied with the connector differs from the CA Top Secret supplied exit with the addition of three calls to external programs.

To deactivate the exit, run the following command:

```
'F TSS,EXIT(OFF)'
```

3.3.2 Integrating Exits

Note: If there are other exits installed on Top Secret, then perform the procedure described in this section.

If one or more third-party modules have been installed with the Top Secret (TSSINSTX) exit, then integration is required. This integration may be accomplished through code modification of either the Reconciliation Agent exit or the third-party exit.

This section discusses the following topics:

- Working with the Reconciliation Agent Exit Source
- Integrating the Reconciliation Agent Exit with Other Exits

3.3.2.1 Working with the Reconciliation Agent Exit Source

The Reconciliation Agent exit can be modified in a number of different ways to integrate it with existing Top-Secret exits. To facilitate this alteration, the source for the exit is provided in the maclib.xmi file.

Note: This procedure should be undertaken only by experienced mainframe programmers. The exit runs in z/OS supervisor mode, and appropriate precautions should be taken before modifying the exit.

To work with the exit source:

1. Upload the maclib.xmi file in binary format to the mainframe using Option #6 on TSO.
2. After the upload is completed, run the following TSO command:

   ```
   RECEIVE da('filename upload')
   ```

3. When prompted, specify the dataset name IDF.MACLIB.CNTL.
4. The maclib.xmi file contains TSSINSTX, which is the source and macros for the standard exit. These are used for assembly and linkedit of the installable binary. You must customize the TSSINSTX DD SYSLIB as follows:

   ```
   // SYSLIB DD DISP=SHR,DSN=SYS1.MACLIB
   //        DD DISP=SHR,DSN=SYS1.MODGEN
   //        DD DISP=SHR,DSN=SYS1.AMODGEN
   //        DD DISP=SHR,DSN=CAI.TSSOPMAT
   //        DD DISP=SHR,DSN=IDF.MACLIB.CNTL
   ```

   The SYS1 libraries are z/OS libraries and the CAI is the Top Secret Maclib containing the exit macros. The IDF.MACLIB.CNTL is created by the RECEIVE command and contains the copybooks required for assembly.
5. Change the following Assemble and Linkedit parameter:

   ```
   //AL PROC LMOD='IDF.LINKLIB',
   ```

   This parameter in the predefined z/OS procedure uses an LMOD parameter, which is the name of the Loadlib for the destination of the exit module. During installation, you assemble and linkedit to this library, and then (optionally) APF authorize the library. Typically, the library resides in the Linklist. If this is true for your operating environment, then APF authorization is not required.

3.3.2.2 Integrating the Reconciliation Agent Exit with Other Exits

---

Note: Modifications similar to the ones performed on the Reconciliation Agent exit can be performed on the third-party exit. However, the exact procedure depends on the content of the third-party exit.

Only one module is called as the Top Secret Exit (TSSINSTX). All other exits must either be integrated into a single unified TSSINSTX or renamed so that the modules do not conflict.

Integration of the Reconciliation Agent exit can be accomplished in one of the following ways:

- Using the Reconciliation Agent Exit As First Executed with Another Exit
- Using Reconciliation Agent Exit As Last Executed with Another Exit

> **Note:** It is recommended that the Reconciliation Agent exit be called last, or be the only exit. This is because other exits might modify data. If this occurs after the Reconciliation Agent exit has been called, then the Oracle Identity Manager data repository is not completely synchronized with the Top Secret repository.

- Using the Reconciliation Agent Exit as the One Executed Between Other Exits

3.3.2.2.1 Using the Reconciliation Agent Exit As First Executed with Another Exit

> **Note:** Because the modification to the Reconciliation Agent exit code is in the exit section, the other exit code will be called after execution of the Reconciliation Agent exit code.

To use the Reconciliation Agent exit as the first executed with another exit:

1. Deactivate the currently installed TSSINSTX by running the following command:

   ```
   F TSS,EXIT(OFF)
   ```

2. Rename the installed TSSINSTX as TSSEXIT in the appropriate load library.

3. Modify the Reconciliation Agent exit as follows:

   a. Insert the following instructions immediately after the exit label:

   ```
   EXIT DS 0H
   LA R1,R9           Copy parmlist ptr to Reg1(R1)
   LR R11,R13         Save TSS's savearea PTR
   LA R13,WORKAREA
   L  R15,=V(TSSEXIT) Load Reg15 with address of TSSEXIT
   BALR R14,R15
   LTR  R15,R15
   LM   R0,R14,0(R13)
   BR   R14           End
   ```

   b. Save the modified exit in the installation TSS Product library.

   c. Customize and run the JCL provided in IDF.JCLLIB member ASMINSTX.

   This will assemble and linkedit the customized TSSINSTX exit.

   d. Verify that TSSINSTX is assembled with an MVS condition code of all 0000.

   e. If the TSS product library is in the Linklist, refresh it by running the following command:

   ```
   F LLA,REFRESH
   ```

   f. After the refresh is completed, activate the new exit by running the following command:

   ```
   F TSS,EXIT(ON)
   ```

3.3.2.2.2 Using Reconciliation Agent Exit As Last Executed with Another Exit

Note: Because the modification to the Reconciliation Agent exit code is performed in the PREINIT section, the other exit code will be called before execution of the Reconciliation Agent exit code.

To use the Reconciliation Agent exit as the last executed with another exit:

1. Deactivate the currently installed TSSINSTX by running the following command:

   ```
   F TSS,EXIT(OFF)
   ```

2. Rename the installed TSSINSTX as TSSEXIT in the appropriate load library.
3. Modify the Reconciliation Agent exit as follows:

   a. Change the ##MATRIX byte for PREINIT to a value of #####YES.

   b. Insert the following instructions immediately after the PREINIT label:

   ```
   LA R1,R9           Copy parmlist ptr to Reg1(R1)
   LR R11,R13         Save TSS's savearea PTR
   LA R13,WORKAREA
   L  R15,=V(TSSEXIT) Load Reg15 with address of TSSEXIT
   BALR R14,R15
   B  PASSPASS        Branch to continue
   ```

   c. Save the modified exit into the installation TSS Product library.

   d. Customize and run the JCL provided in IDF.JCLLIB member ASMINSTX.

   This will assemble and linkedit the customized TSSINSTX exit.

   e. Verify TSSINSTX assembled with an MVS condition code of all 0000

   f. If the TSS product library is in the Linklist, refresh it by running the following command:

   ```
   F LLA,REFRESH
   ```

   g. After the refresh is completed, activate the new exit by running the following command:

   ```
   F TSS,EXIT(ON)
   ```

3.3.2.2.3 Using the Reconciliation Agent Exit as the One Executed Between Other Exits

By combining the changes described for the first executed and last executed exits, you can configure the Reconciliation Agent exit to be called in the middle of the execution stack.

3.4 Configuring TCP/IP Connection and Starter Tasks

This section describes how to establish a TCP/IP connection with the LDAP Gateway and the building and operation of the starter tasks in the following topics:

- Establishing a Connection With the LDAP Gateway
- Building and Operation of the Starter Tasks

Note:

- Events detected by the Reconciliation Agent through exit technology are transformed into messages and encrypted using AES encryption before being passed to the LDAP Gateway.
- If the LDAP Gateway is not running, then messages are held until the Gateway is returned to service and also secured in an AES-encrypted file on the mainframe. These messages are sent when the LDAP Gateway resumes running.
- If the subpool is stopped by an administrator, then it shuts down the Provisioning Agent, thereby destroying any messages that are not transmitted. However, the messages in the AES-encrypted file are not affected and can be recovered.

3.4.1 Establishing a Connection With the LDAP Gateway

This section describes how to configure TCP/IP as the message transport layer. Check with the systems programmer for detailed information about using TCP/IP. The objective 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.

To establish a TCP/IP connection with the LDAP Gateway:

1. Start the LDAP Gateway.

   Note: For instructions to start and stop the LDAP Gateway, see "Installing and Configuring the LDAP Gateway" on page 2-8.

2. 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 start 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 the mainframe
- IP address for the router
- IP addresses for domain name servers

Note: To use TCP/IP as the message transport layer, you might need the help of the systems programmer to create ports on the mainframe and to provide security authorizations.

The Provisioning Agent and Reconciliation Agent JCL procedure shipped with the connector must be edited to specify the user parameters that are different for each environment. To edit the Provisioning Agent and Reconciliation Agent JCL, you must edit the Voyager and Pioneer started tasks (STCs) procedures. To do so:

1. Change the value for PARM='TCPN=TCPIP' to the name of the running TCP/IP started task.

2. Change the IP address to the address (IPAD= parameter) of the LDAP Gateway (for Voyager only).
3. Change the port number (PORT= parameter) to the port assigned in the LPAR (z/OS system) from which the Provisioning Agent will be listening on for messages from the LDAP Gateway.
4. Change the port number (PORT = parameter) to the port that the LDAP gateway is listening on for messages from the Reconcilation Agent (Voyager).
5. For Voyager Reconciliation Agent, TSO edit the VOYAGERX procedure as shown:

```
//VOYAGERX EXEC PGM=VOYAGERX,REGION=0M,TIME=1440,
//    PARM=('TCPN=TCPIP',
//          'IPAD=&SERVER',  ------ This must match the IP address or the DNS
                             ------ host name of the LDAP Gateway.
//          'PORT=&PORT',    ----- Port must be 5190.
//          'DEBUG=N',
//          'ESIZE=16',
//          'DELAY=10',
//          'STARTDELAY=10',
//          'PRTNCODE=SHUTRC')
//STEPLIB  DD DISP=SHR,DSN=IDF.LINKLIB   ------This is not required for
Linklist.
//         DD DISP=SHR,DSN=TCPIP.SEZATCP
//CACHESAV DD DSN=VOYAGER.CACHESAV,DISP=SHR
//DEBUGOUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//
```

Where:

- ESIZE=16 is used to denote AES encryption.
- DELAY=01 to 99 in seconds. This is used for Top Secret cache. The value of DELAY is 10 on most z/OS systems running CA Top Secret.
- STARTDELAY=10 is the recommended value (in seconds).
- PRTNCODE=SHUTRC shows all MVS condition codes after the Reconciliation Agent shuts down.
- PRTNCODE=SHUTRC shows all MVS condition codes after the Reconciliation Agent shuts down. Alternatively, PRTNCODE=TERMRC shows an MVS condition code of 0000 (signifying successful completion) after the Reconciliation Agent shuts down.
- IPAD= is either the IP address or the DNS hostname of the LDAP Gateway.
- DEBUG=Y routes debugging statements to the DEBUGOUT data definition statement (DD).

  > **Caution:** This setting generates a large amount of output. It is recommended that you consult support personnel before you use apply this setting.

> **Note:** To shut down the Reconciliation Agent, run the following command from the z/OS operator's console:
>
> ```
> 'F VOYAGER,SHUTDOWN'
> ```
>
> To shut down the Provisioning Agent, run the following command from the z/OS operator's console:
>
> ```
> 'F PIONEER,SHUTDOWN'
> ```

- TCPN=TCPIP is the name of TCPIP STC name.
- DEBUG can be one of the following for both the Reconciliation Agent and Provisioning Agent:
  - N is for no debugging output.
  - Y is for debugging output.
  - Z is for detailed debugging.

> **Note:** If the "data set in use" message is displayed when you attempt to edit a member, then press the F1 key twice to see details of the member that you are trying to edit. The name of the job that is causing the exception is displayed. On the z/OS console, you can remove the job by using the `p` or the `c` command.

Apply the following guidelines while working with the Reconciliation Agent:

- The subpool (RUNSTART.JCL) must be started before starting the Reconciliation Agent. The subpool is used as an in-memory storage for message creation.
- Because you are using TCP/IP, the LDAP Gateway must be started first. If the Reconciliation Agent is started first, then an error is generated with RETCODE=-01 and ERRORNO=61 because the LDAP Gateway is not available.

Voyager Cachesav dataset:

Pre-allocate the Cachesav dataset of the Voyager Reconciliation Agent with the following dataset attributes:

```
DSORG=PS, LRECL=32, RECFM=FB, BLKSIZE=27968, CYLS = 5
```

For Pioneer Provisioning Agent:

```
//PIONEER  EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//        PARM=('TCPN=TCPIP',
//                     'IPAD=0.0.0.0',
//                     'PORT=5790',
//                     'DEBUG=N',
//                     'ESIZE=16',
//                     'LPAR=XXXXXXXX')
//STEPLIB      DD  DSN=IDF.LINKLIB ,DISP=SHR
//SYSPRINT   DD SYSOUT=*
//SYSPUNCH DD  SYSOUT=(*,INTRDR)
//DEBUGOUT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
```

Where:

- TCPN=TCPIP is the name of TCPIP STC name.
- IPAD must always be zeros.
- PORT=5790 must match the provisioning port of the LDAP Gateway.
- ESIZE=16 must be left as is.
- LPAR= 'XXXXXXXX' . This is a 8 character unique identifier for the system partition on which the Provisioning Agent is running.

3.4.2 Building and Operation of the Starter Tasks

There are two different JCLs to set up and run the Provisioning Agent and Reconciliation Agent. There is a JCL member for each agent. RUNPIONX and RUNVOYAX are samples to set up the started tasks.

The parameters for RUNPIONX are:

- TCPN: Name of the TCP process
- IPAD: IP address of the computer on which the Provisioning Agent is running
- PORT: Incoming connection port for the Provisioning Agent
- DEBUG: Debug switch for showing the extra output
- ESIZE: AES encryption used

The parameters for RUNVOYAX are:

- TCPN: Name of the TCP process
- IPAD: IP address of the computer on which the Reconciliation Agent is connected
- PORT: Outgoing connection port for the Reconciliation Agent
- DEBUG: Debug switch for generating large amount of output into the z/OS JES2 queue that facilitates troubleshooting
- ESIZE: AES encryption used

The source code for each program is as follows:

For RUNPIONX:

Note: The BATJINFO, VSAMGETO, and VSAMGETU data definition (DD) statements are not required on Top Secret installations and can be commented out as shown in this block of code.

```
//PIONEERX EXEC PGM=PIONEERX,REGION=0M,TIME=1440,
//  PARM=('TCPN=TCPIP',
//     'IPAD=&SERVER',
//     'PORT=&PORT'
//     'DEBUG=Y',
//     'ESIZE=16',
//     'LPAR=TOPSECRET-SYS')

//    'LPAR= name ')
//STEPLIB DD DISP=SHR,DSN=IDF.LINKLIB
//     DD DISP=SHR,DSN=TCPIP.SEZATCP
//* BATJINFO DD DISP=SHR,DSN=hlq.BATJCARD
//* VSAMGETU DD DISP=SHR ,DSN=hlq.SWUSERS
//* VSAMGETO DD DISP=SHR,DSN=hlq.TOPSCOUT
//SYSPRINT DD SYSOUT=X
//DEBUGOUT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=X
//
```

Note: In the code, hlq stands for installation high-level qualifier. The IPAD= parameter above must always be `0.0.0.0`.

For RUNVOYAX:

```
//VOYAGERX EXEC PGM=VOYAGERX,REGION=0M,TIME=1440,
//    PARM=('TCPN=TCPIP',
//          'IPAD=&SERVER',          ß--- must match LDAPS IP address
//          'PORT=&PORT',             ß---  must be Port 5190
//          'DEBUG=Y',
//          'ESIZE=16',
//          'DELAY=00',
//          'STARTDELAY=10',
//          'PRTNCODE=SHUTRC')
//STEPLIB  DD DISP=SHR,DSN=IDF.LINKLIB    ß- not required for Linklist
//         DD DISP=SHR,DSN=TCPIP.SEZATCP
//CACHESAV DD DSN=VOYAGER.CACHESAV,DISP=SHR
//DEBUGOUT DD SYSOUT=*
//SYSPRINT DD SYSOUT=X
//SYSUDUMP DD SYSOUT=X
//
```

For the Reconciliation Agent:

The dataset attributes for Cachesav is:

```
Cachesav         -       DSORG(PS),LRECL=(32),RECFM=(FB),BLKSIZE=(27968)
```

4 Configuring the Connector

The connector enables real-time reconciliation of user data from the target system. After you deploy the connector and import existing user data from the target system to Oracle Identity Manager, you need not depend on a scheduled task to initiate reconciliation runs with the target system.

This chapter discusses the following topics:

- Configuring Trusted Source Reconciliation
- Configuring Limited Reconciliation
- Running Initial Reconciliation
- Configuring Account Status Reconciliation
- Adding New Fields for Provisioning

4.1 Configuring Trusted Source Reconciliation

The XML file for trusted source reconciliation, oimTopSecretTrustedXellerateUser.xml, contains definitions of the connector components that are used for trusted source reconciliation. To import this XML file:

> **Note:** The procedure described in this section enables trusted source reconciliation for both the initial reconciliation run and subsequent real-time reconciliation runs.

1. Open the Oracle Identity Manager Administrative and User Console.
2. Click the **Deployment Management** link on the left navigation pane.
3. Click the **Import** link under Deployment Management. A dialog box for opening files is displayed.
4. Locate and open the oimTopSecretTrustedXellerateUser.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 **Import**.
8. In the message that is displayed, click **Import** to confirm that you want to import the XML file, and then click **OK**.

4.2 Configuring Limited Reconciliation

By default, all target system records that are added or modified after the last reconciliation run are reconciled during the current reconciliation run. You can specify the subset of newly added or modified target system records that must be reconciled. You do this by using the _resourceObject_ parameter in the initialTopSecretAdv.properties file.

> **Note:** The "Running Initial Reconciliation" section provides information about the initialTopSecretAdv.properties file.

You use the _resourceObject_ parameter to specify the resource object that you want to use during reconciliation. You might have created multiple resource objects to represent multiple user types in your organization. You can enter more than one resource object in the value of the _resourceObject_ parameter. In addition, you can include TSS attribute-value pairs to filter records for each resource object.

The following is a sample format of the value for the _resourceObject_ parameter:

```
_resourceObject_:[ATTRIBUTE1:VALUE1]RESOURCE_OBJECT1,[ATTRIBUTE2:VALUE2]RESOURCE_O
BJECT2, . . .
```

As shown in the sample format, specifying a filter attribute is optional. If you do not specify a filter attribute, then all records for that resource object are reconciled.

Apply the following guidelines while specifying a value for the _resourceObject_ parameter:

- The names of the resource objects must be the same as the names that you specified while creating the resource objects by using the Design Console.
- The TSS attribute names must be the same as the names used in the LDAP gateway configuration files.

  See Also: The "Installing and Configuring the LDAP Gateway" section for information about the LDAP gateway configuration files

- The value must be a regular expression as defined in the java.util.regex Java package. Note that the `find` methodology of the regex matcher is used rather than the `matches` methodology. This means that a substring matching rule can be specified in the pattern, rather than requiring the entire string matching rule.
- Multiple values can be matched, with each individual value being separated by a vertical bar (|). For example:

  ```
  [ATTRIBUTE:VALUE1|VALUE2|VALUE3]RESOURCE_OBJECT
  ```

- Multiple filters can be applied to the attribute and to the same resource object. For example:

  ```
  [ATTRIBUTE1:VALUE1]&[ATTRIBUTE2:VALUE2]RESOURCE_OBJECT
  ```

The following is a sample value for the _resourceObject_ parameter:

```
_resourceObject_:(tso.holdclass:X)TSSR01,(category:value1|value2|value3)TSSResourc
eObject2,(tso)TSSResourceObject24000,Resource
```

In this sample value:

- `(tso.holdclass:X)TSSRO1` represents a user with `X` as the attribute value for the TSO Holdclass segment. Records that meet this criterion are reconciled with the TSSRO1 resource object.
- `(category:value1|value2|value3)TSSResourceObject2` represents a user with `value1`, `value2`, or `value3` as their category. Records that meet this criterion are reconciled with the TSSResourceObject2 resource object.
- `(tso)TSSResourceObject24000` represents a user with TSO privileges. A TSO attribute value is not specified. Records that meet this criterion are reconciled with the TSSResourceObject24000 resource object.
- All other records are reconciled with the Resource resource object.

4.3 Running Initial Reconciliation

The initial reconciliation run involves importing user data from the target system into Oracle Identity Manager, immediately after you deploy the connector.

To start the initial reconciliation run:

1. Ensure that properties that are common to both the run script and the run_initial_recon_provisioning script have the same values.

   The run script is in the *LDAP_INSTALL_DIR*/bin directory. The run_initial_recon_provisioning script is in the *OIM_HOME*/xellerate/JavaTasks directory.

2. In a text editor, open the *OIM_HOME*/xellerate/JavaTasks/initialTopSecretAdv.properties file.

3. In the initialTopSecretAdv.properties file, specify values for the parameters that control the initial reconciliation script.

   > **Note:** Ensure that properties that are common to both the initialTopSecretAdv.properties file and topsecretConnection.properties file have the same values.

   Specify values for the following parameters in the initialTopSecretAdv.properties file:

   - xlAdminId: Oracle Identity Manager administrator ID.
   - idfTrusted: Enter `true` as the value of this property to specify that you want to perform trusted source reconciliation with the target system. Enter `false` to specify target resource reconciliation.
   - _resourceObject_: Resource object for reconciliation. See "Configuring Limited Reconciliation" for information about specifying a value for this parameter.
   - _itResource_: IT resource for target resource reconciliation.
   - _dummyPwd_: Dummy password for initial reconciliation.
   - isFileRecon: The value for this is `true`, which specifies file-based initial reconciliation. You must not change this value.
   - userFile: Enter the name of the TXT file in which you have stored the user IDs of the target system users that you want to reconcile. This file must be placed in the following directory:

     ```
     OIM_HOME/xellerate/JavaTasks
     ```

For more information about this file, see the sample user.txt file in the scripts directory on the installation media.

- #REMOVED: Ignore this property.
- reconAttrs: Fields that are reconciled.
- tsoReconAttrs: TSO fields that are reconciled.
- idfServerUrl: Enter the LDAP Gateway host and port.

You must not change the values of the remaining properties in the initialTopSecretAdv.properties file.

The following is a sample set of values for the properties in the initialTopSecretAdv.properties file:

```
xlAdminId:xelsysadm
idfTrusted:false
_resourceObject_:OIMTopSecretResourceObject
_itResource_:TopSecretResource
_dummyPwd_:Pwd123
isFileRecon:true
userFile:user.txt
#REMOVED: sn,givenName,revoke,identificationUID,cicsid,minDays,maxDays,prefix,
reconAttrs:uid,cn,userPassword,department,instdata,division,lastModificationDat
e,createDate,type
tsoReconAttrs:tsolacct,tsohclass,tsojclass,tsomclass,tsolproc,tsolsize,tsomsize
,tsosclass,tsounit,tsoudata,tsocommand,tsodest,tsolopt
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
```

4. In a text editor, open the *OIM_HOME*/xellerate/JavaTasks/run_initial_recon_provisioning script.

5. To perform trusted source reconciliation:

   Note: Ignore step 5 if you want to run target resource reconciliation only.

   a. Set the value of the JV parameter in the script to -*X* to reconcile Xellerate User.

   b. Run the script.

   When you run the script, it opens the file (whose name is the value of the userFile property) containing user data and reads the user IDs of the users that you want to reconcile. Then, the loader, which is the initial load script, connects to the LDAP Gateway and issues commands to fetch the required user data from the target system. This data is loaded in the LDAP Gateway cache and reconciliation events are submitted to Oracle Identity Manager. OIM

User records are created for all the target system users identified by the userFile property in the initialTopSecretAdv.properties file.

c. In the run_initial_recon_provisioning script, change the value of the JV parameter to `-R` to run target resource reconciliation.

d. Run the script again.

Because you have set the value of the JV parameter in the script to `-R`, target resource reconciliation is performed when you run the script. Resources are assigned to each OIM User that was created when you first ran the script.

6. To perform target resource reconciliation only:

> **Note:** Ignore step 6 if you want to run trusted source reconciliation.

a. In a text editor, open the initialTopSecretAdv.properties file and enter `false` as the value of the idfTrusted property to specify that you want to perform target resource reconciliation with the target system.

Make the same change in the topsecretConnection.properties file.

b. In the run_initial_recon_provisioning script and change the value of the JV parameter to `-P` to run target resource reconciliation.

c. Run the script again.

Because you have set the value of the JV parameter in the script to `-P`, target resource reconciliation is performed when you run the script.

After the initial reconciliation run ends, real-time reconciliation takes over and newly created or modified user data is automatically reconciled into Oracle Identity Manager.

If a problem exists with fault tolerance and the LDAP Gateway and Reconciliation Agent are down for a long time, and if there is a possibility of losing user data, then run full reconciliation.

4.4 Configuring Account Status Reconciliation

When a user's account is disabled or enabled on the target system, the user is reconciled and the changed status is reflected in Oracle Identity Manager. To configure the reconciliation of account status data:

1. In the *LDAP_INSTALL_DIR*/topsecretConnectrion.properties file, add the name of the status field to the reconAttrs section.

   Make the same change in the initialTopSecretAdv.properties file, which is in the *OIM_HOME*/xellerate/JavaTasks directory.

2. Restart the LDAP Gateway for the changes to take effect.

3. In the Design Console:

   > **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about the following steps

   - In the OIMTopSecretResourceObject resource object, create the Status reconciliation field.
   - In the OIMTopSecretProvisioningProcess process definition, map the field for the Status field to the OIM_OBJECT_STATUS field.

4.5 Adding New Fields for Provisioning

To add a new field for provisioning to CA Top Secret:

> **See Also:** *Oracle Identity Manager Design Console Guide* for detailed information about these steps

1. Log in to the Oracle Identity Manager Design Console.
2. Expand the **Development Tools** folder.
3. Double-click **Form Designer**.
4. Search for and open the CA Top Secret main process form, such as the UD_TOPS_ADV_MODEL process form.
5. Click **Create New Version**, and then click **Add**.
6. Enter the details of the field. For example, if you are adding the uid field, then enter USER in the Name field, and then enter the rest of the details of this field.
7. Click **Save**, and then click **Make Version Active**.
8. Expand the **Administration** folder.
9. Double-click **Lookup Definition**.
10. Add the new Attribute Form column name to the AtMap.TopSecret lookup definition. For example, Code Key value is UD_TOPS_ADV_MODEL and Decode value is model. The Code Key value is the column name in the CA Top Secret main process form, and the Decode value is the name of the field on the target CA Top Secret system, which maps to the corresponding LDAP field name.
11. If you want to add an update process task for a new custom field in Oracle Identity Manager, create a new process task associated with the Oracle Identity Manager field by using the adpMODIFYUSER adapter for CA Top Secret.

5 Troubleshooting

This chapter contains the following sections:

5.1 Troubleshooting

Table 5–1 lists solutions to some commonly encountered issues associated with the connector.

> **Note:** Verify that you have performed Step 11 of the procedure described in the "Installing and Configuring the LDAP Gateway" section to enable logging.

Table 5–1 Troubleshooting

Problem Description	Solution
Oracle Identity Manager cannot establish a connection to the CA Top Secret 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 LDAP 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 IP address of the server that hosts the LDAP Gateway, is configured in the Reconciliation Agent JCL. ■ View the LDAP 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 account 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 LDAP Gateway. ■ If any of the mainframe JCL jobs have reached an abnormal end, then make the required corrections and rerun 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 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.
The LDAP Gateway fails and stops working	If this problem occurs, then the Reconciliation Agent stops sending messages to the LDAP Gateway. Instead, it stores them in the subpool cache. When this happens, restart the LDAP Gateway instance so that the Reconciliation Agent reads the subpool cache and resends the messages.
The LDAP Gateway is running. However, the Reconciliation Agent fails and stops working	If this problem occurs, then all events are sent to the subpool cache. If the mainframe fails, then all messages are written to the disk. When this happens, restart the Reconciliation Agent instance so that it reads messages from the disk or subpool cache and resends the messages.

5.2 Guidelines on Using the Connector

Apply the following guidelines while using the connector:

- The 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.

> **Caution:** To avoid errors of this type, 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 related to passwords on mainframes. These passwords are also subject to restrictions imposed by corporate policies and rules about mainframe passwords.
- If you configure the connector for trusted source reconciliation and set the idfTrusted property in the initialTopSecretAdv.properties file to `true` on one of the target system installations on the mainframe, then it must be set to `true` on all installations that connect to the same LDAP Gateway. Otherwise, the connector will fail. This applies only to a configuration in which a single LDAP Gateway connects to multiple installations of the target system.

6

Known Issues

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

- **Bug 6668844**

  If there is any reconciliation field mapped to the OIM_OBJECT_STATUS field in the process definition, then the associated process form cannot be modified to create a new version. To create a new version of the process form, remove the reconciliation field mapping of OIM_OBJECT_STATUS from the process definition, update the process form, and then remap the OIM_OBJECT_STATUS field.

- **Bug 6904041**

  Group membership changes of user profiles that are updated on the target system cannot be reconciled into Oracle Identity Manager.

- **Bug 7033009**

  The number sign (#) or a space at the *beginning* of the User Profile ID string is not supported. In addition, the following characters are not supported in the User Profile ID string:

  - Comma (,)
  - Plus sign (+)
  - Double quotation mark (")
  - Slash (/)
  - Left angle bracket (<)
  - Right angle bracket (>)
  - Backslash (\)

Index