Oracle® Identity Manager

Connector Guide for CA Top Secret Advanced

Release 9.0.4

E10424-23

August 2018

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

E10424-23

Primary Author: Balakrishnan Nanjan

Contributing Authors: Prakash Hulikere, Vagdevi Jayashankar, Binika Kumar

Contents

2 Connector Deployment on Oracle Identity Manager

3 Connector Deployment on the Mainframe

4 Using the Connector

5 Extending the Functionality of the Connector

List of Figures

List of Tables

Preface

This guide describes the connector that is used to integrate Oracle Identity Manager with CA Top Secret.

Audience

This guide is intended for resource administrators and target system integration teams. Installation of the connector components on the mainframe requires experience with CA Top Secret and various z/OS technologies and components, including TCP/IP, QSAM (flat files), and z/OS libraries.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For information about installing and using Oracle Identity Manager, see the Oracle Identity Manager documentation library.

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

The following Oracle Technology Network page provides links to Oracle Identity Manager documentation:

`http://docs.oracle.com/cd/E11223_01/index.htm`

Documentation Updates

Oracle is committed to delivering the best and most recent information available. For information about updates to the Oracle Identity Manager Connectors documentation, 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 Advanced Connector for CA Top Secret?

This chapter provides an overview of the updates made to the software and documentation for the Oracle Identity Manager Advanced Connector for CA Top Secret in release 9.0.4.20.

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 sections discuss software updates:

- Software Updates in Release 9.0.4.20
- Software Updates in Release 9.0.4.19
- Software Updates in Release 9.0.4.18
- Software Updates in Release 9.0.4.17
- Software Updates in Release 9.0.4.16
- Software Updates in Release 9.0.4.15
- Software Updates in Release 9.0.4.14
- Software Updates in Release 9.0.4.13
- Software Updates in Release 9.0.4.12
- Software Updates in Release 9.0.4.11
- Software Updates in Release 9.0.4.7
- Software Updates in Release 9.0.4.6
- Software Updates in Release 9.0.4.5
- Software Updates in Release 9.0.4.4
- Software Updates in Release 9.0.4.3
- Software Updates Up To Release 9.0.4.2

Software Updates in Release 9.0.4.20

The following are the software updates in release 9.0.4.20:

- End of Life Support for Trusted Source Reconciliation
- Support for Oracle Identity Manager Release 11.1.2.3.0
- Resolved Issues in Release 9.0.4.20

End of Life Support for Trusted Source Reconciliation

From this release onward, the connector no longer supports trusted source reconciliation. Only target resource reconciliation is supported.

Support for Oracle Identity Manager Release 11.1.2.3.0

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* Release 2 PS3 (11.1.2.3.0).

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Resolved Issues in Release 9.0.4.20

The following table lists issues resolved in release 9.0.4.20:

Bug Number	Issue	Resolution
18962680	The Code Key and Decode values of the Lookup.ProfileNames lookup definition used a dash (-) instead of a tilde (~).	This issue has been resolved.
20270833	CICSOPCLASS mapped incorrectly when reconciled through VOYAGER.	This issue has been resolved.

Software Updates in Release 9.0.4.19

The following are the software updates in release 9.0.4.19:

- Support for Three New VOYAGER Enhancements
- Addition of STARTUP and WRAPUP
- Support for New PIONEER Enhancement
- Support for VOYAGER AUDIT Log
- Resolved Issues in Release 9.0.4.19

Support for Three New VOYAGER Enhancements

From this release onward, the connector supports the following VOYAGER enhancements:

1. MSGID01=<YES | NO>,IDMV602E,xx - for LDAP recovery message suppression.
2. RECOVERY_INTERVAL=xxx,<MINS | SECS> - recovery interval for IP addresses.
3. DNS_RECOVERY_INTERVAL=xxx,<MINS | SECS> - recovery interval for DNS addresses.

Addition of STARTUP and WRAPUP

From this release onward, STARTUP and WRAPUP have been added back as the method of creating the Subpool for VOYAGER and deleting the Subpool. The VOYAGER control file parameter (SUBPOOL_SIZE=) is no longer supported.

Support for New PIONEER Enhancement

From this release onward, the connector supports a new PIONEER enhancement. EXPORT_MON=YES, REC=01000 – CFILE transfer monitor while PIONEER is running.

Support for VOYAGER AUDIT Log

From this release onward, the VOYAGER Audit log, turned on with VOYAGER parameter AUDIT_LOG=YES has been enhanced to show ACID being processed as well as the number of items or messages read from the Subpool.

Resolved Issues in Release 9.0.4.19

The following table lists issues resolved in release 9.0.4.19:

Bug Number	Issue	Resolution
18950032	High-availability reconciliation was not supported for users who were deleted from the internal LDAP store.	This issue has been resolved. High-availability reconciliation of deleted internal LDAP users is now supported.
18231514	CFILE XML error messages were not logged to the main LDAP gateway log file.	This issue has been resolved. CFILE XML error messages are now logged to both the XML error log and main LDAP gateway log file.
19239326	The LDAP Gateway server returned a generic exception when granting a duplicate entitlement to a user.	This issue has been resolved. Support for error code 64, User Already Linked to Group/Profile, has been added to all provisioning functions that grant an entitlement to a user.
19316338	The LDAP gateway lacked support for reconciling the display name of a ZONE to which a user belongs.	This issue has been resolved. The LDAP gateway now supports both scheduled task and real-time reconciliation of the ZONE display name attribute and value.
19308581	The LDAP gateway did not correctly format a TSOCOMMAND value containing spaces or single quotation marks.	This issue has been resolved. The LDAP gateway now properly formats a TSOCOMMAND value that contains a space character, single quotation mark, or both.

Software Updates in Release 9.0.4.18

The following are the software updates in release 9.0.4.18:

- Support for New Oracle Identity Manager Release
- Resolved Issues in Release 9.0.4.18

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11g release 2 (11.1.2.0.1) or later. Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Resolved Issues in Release 9.0.4.18

The following table lists issues resolved in release 9.0.4.18:

Bug Number	Issue	Resolution
16828743	Users reconciled to Oracle Identity Manager using the CFILE XML processing feature did not include all permission data needed to certify in accordance with SOX.	This issue has been resolved. Users and profiles reconciled using the CFILE XML processing feature will now include all necessary permission data required to certify in accordance with SOX.
17628090	Mainframe agent log messages did not contain a date, timestamp, or message code. Messages produced by the mainframe were not described in the documentation.	This issue has been resolved. Documentation has been updated to better describe mainframe log messages. Where applicable, date, timestamp, and message codes have been added to the mainframe log messages.
16925326	The 9.0.4.17 connector XML throws an error when importing the connector.	This issue has been resolved. The 9.0.4.18 XML no longer throws any errors during connector import or connector upgrade operations.
16855865	The run script used to start the LDAP gateway did not add the correct Oracle Identity Manager libraries to the classpath.	This issue has been resolved. The LDAP gateway run script now adds the correct Weblogic and Oracle Identity Manager libraries to the classpath.

Software Updates in Release 9.0.4.17

The following are the software updates in release 9.0.4.17:

- Support for Scheduled Task – Reconcile Deleted Users to Oracle Identity Manager
- Support for Scheduled Task – Reconcile Users to Internal LDAP
- Support for Scheduled Task – Reconcile LDAP Users to Oracle Identity Manager
- Support for LU6.2 Attributes During Provisioning and Reconciliation Operations
- Support for Top Secret RENAME Provisioning Operation
- Support for Top Secret GENCERT Provisioning Operation
- Support for Top Secret GENREQ Provisioning Operation
- Support for Configurable Property for Revoking PSUSPEND Users
- Support for Configurable Lookup Code Name in Scheduled Tasks
- Support for Pioneer and Voyager Parameters in a Control File
- Support for New Pioneer Function for LDAP
- Removal of STARTUP and WRAPUP
- Support for a New Pioneer-Message Function in Voyager
- Resolved Issues in Release 9.0.4.17

Support for Scheduled Task – Reconcile Deleted Users to Oracle Identity Manager

From this release onward, the connector supports an additional scheduled task for reconciling deleted users on the target system. This task retrieves a list of users from the target system and compares that list with a list of users from Oracle Identity Manager. If a user is found to exist within Oracle Identity Manager, but not on the target system, then a delete reconciliation event for the user is sent to Oracle Identity Manager. See Section 4.4.2.2, "Top Secret Reconcile Deleted Users to OIM" for more details.

Support for Scheduled Task – Reconcile Users to Internal LDAP

From this release onward, the connector supports an additional scheduled task for reconciling users on the target system to the internal LDAP store. This task retrieves a list of users and their profiles from the target system and reconciles each user to the internal LDAP gateway metastore. See Section 4.4.2.3, "Top Secret Reconcile Users to Internal LDAP" for more details.

Support for Scheduled Task – Reconcile LDAP Users to Oracle Identity Manager

From this release onward, the connector supports an additional scheduled task for reconciling users from the internal LDAP store to Oracle Identity Manager. This task retrieves a list of users from the internal LDAP store and reconciles those users to Oracle Identity Manager. See Section 4.4.2.4, "Top Secret Reconcile All LDAP Users" for more details.

Support for LU6.2 Attributes During Provisioning and Reconciliation Operations

From this release onward, the connector supports provisioning and reconciliation of LU6.2 attributes. Specifically, support for the #APPL, #ENTITY, BC1CHAIN, BC2CHAIN, SET1DISP, and SET2DISP attributes has been added to TSS CREATE, ADDTO, REPLACE, REMOVE, and LIST commands.

Support for Top Secret RENAME Provisioning Operation

From this release onward, the connector supports the RENAME Top Secret operation. See Section 1.5.1, "Supported Functions for Target Resource Reconciliation" and Section 1.5.2, "Supported Functions for Provisioning" for more details.

Support for Top Secret GENCERT Provisioning Operation

From this release onward, the connector supports provisioning of the GENCERT Top Secret operation. See Section 1.5.2, "Supported Functions for Provisioning" and Section 1.5.9, "Provisioning GENCERT Operations" for more details.

Support for Top Secret GENREQ Provisioning Operation

From this release onward, the connector supports provisioning of the GENREQ Top Secret operation. See Section 1.5.2, "Supported Functions for Provisioning" and Section 1.5.10, "Provisioning GENREQ Operations" for more details.

Support for Configurable Property for Revoking PSUSPEND Users

From this release onward, the connector properties file includes a configurable property for revoking users with the PSUSPEND attribute. See Section 2.6, "Installing and Configuring the LDAP Gateway" for more details.

Support for Configurable Lookup Code Name in Scheduled Tasks

From this release onward, the FindAllResources, FindAllDatasets, FindAllProfiles, and FindAllFacilities scheduled tasks include a property called Lookup Code Names. This property is used to specify the lookup code name where results of the task should be stored. See Section 4.2, "Scheduled Tasks for Lookup Field Synchronization" for more details.

Support for Pioneer and Voyager Parameters in a Control File

Support for all Pioneer and Voyager parameters are now contained in a parameter or control file pointed to by "//PARMFLE" ddname on both PIONEER and Voyager. This file can be a QSAM (recfm=f,lrecl=80,blksize=80,dsorg=ps) or a pds member. See Section 3.8, "Configuring the Started Tasks" for more details.

Support for New Pioneer Function for LDAP

A full export of Top-Secret CFILE data will now be done through a conversion utility provided converting it to XML for input into Pioneer. This XML data will be sent to the LDAP on-demand.

Removal of STARTUP and WRAPUP

STARTUP and WRAPUP have been removed. Their functions have been incorporated into Voyager. Voyager has a new SUBPOOL_SIZE= parameter that is used to allocate the CACHE (Subpool) for reconciliation messages.

Support for a New Pioneer-Message Function in Voyager

A new parameter has been added to Voyager, "PIONEER_DELETE_MSGS=YES" or "PIONEER_DELETE_MSGS=NO". This new parameter will force Voyager to process or not process messages originating from Pioneer.

Resolved Issues in Release 9.0.4.17

The following table lists issues resolved in release 9.0.4.17:

Bug Number	Issue	Resolution
16236789	Updates to the UserLogin attribute fails.	This issue has been resolved. Support for the TSS RENAME command is now included.
16266065	Updates to the UserLogin attribute fails.	This issue has been resolved. Support for the TSS RENAME command is now included.
16515205	Single-use password with EXPIRE does not work.	This issue has been resolved. EXPIRE is now a supported attribute in provisioning and reconciliation functions.
16510636	Connector does not include support for both GROUPS and PROFILES operations.	This issue has been resolved. Users can now be provisioned and removed from TSS GROUPS and PROFILES, and their group and profile memberships are now supported during reconciliation.
16240718	Updates to the FullName attribute in OIM are not successfully committed to the mainframe.	This issue has been resolved. The Full Name attribute is now successfully updated in provisioning operations.
15958873	The "Reconcile All Users" scheduled task is not working.	This issue has been resolved. All reconciliation scheduled task functions are now working.

Bug Number	Issue	Resolution
13419640	Maclib.xmi is referenced in the documentation but is not included in the installation media.	This issue has been resolved. Maclib.xmi has been removed from the installation media and is no longer referenced in the documentation.
12675647	Maclib.xmi is referenced in the documentation but is not included in the installation media.	This issue has been resolved. Maclib.xmi has been removed from the installation media and is no longer referenced in the documentation.

Software Updates in Release 9.0.4.16

The following are the software updates in release 9.0.4.16:

- Support for New Reconcile All Users Scheduled Task Properties
- Support for New Feature
- Resolved Issues in Release 9.0.4.16

Support for New Reconcile All Users Scheduled Task Properties

From this release onwards, the connector supports the new All Users scheduled task properties. The TSS Reconcile All Users scheduled task properties have been updated. Users can now customize the UID case during reconciliation, and reconciliation of individual users through the scheduled task is now supported. See Table 4–3 for more details.

Support for New Feature

From this release onwards, the connector supports a new feature. The Oracle Identity Manager reconciliation feature ignoreEvent() is now included. The LDAP Gateway will now confirm whether a reconciliation event should be ignored before creating the event in Oracle Identity Manager. Both real-time reconciliation and full reconciliation utilize this feature. See Section 1.3.2.1, "Full Reconciliation Process" and Section 1.3.2.3, "Incremental (Real-Time) Reconciliation Process" for more details.

Resolved Issues in Release 9.0.4.16

The following table lists issues resolved in release 9.0.4.16:

Bug Number	Issue	Resolution
14048660	The Oracle Identity Manager CA Top Secret connector is unable to reconcile attribute values containing "=" character.	This issue has been resolved. Now the Oracle Identity Manager CA Top Secret connector is allowing "=" characters to be parsed in INSTALLATION-DATA field.
13682327	The reconciliation class name for full user reconciliation is identical for both RACF and Top Secret full user reconciliation.	This issue has been resolved. The reconciliation class name for full user reconciliation can now use with other mainframe connectors.

Bug Number	Issue	Resolution
11795039	The Oracle Identity Manager CA Top Secret connector is unable to reconcile profiles correctly.	This issue has been resolved. The Oracle Identity Manager CA Top Secret connector now allows profiles to be reconciled per user on the child-form.
7359488	The logging is inconsistent in the Oracle Identity Manager CA Top Secret connector.	This issue has been resolved. All logging is using OIM logger in adapters.

Software Updates in Release 9.0.4.15

The following are the software updates in release 9.0.4.15:

- A new *Pioneer Control File Parameter* **QUEUE_DSN=** has been added.
- The value of **JWAIT=** parameter has been changed.
- The value of **RWAIT=** parameter has been changed.

  See Section 3.8, "Configuring the Started Tasks" for more details.

Resolved Issues in Release 9.0.4.15

The following table lists issues resolved in release 9.0.4.15:

Bug Number	Issue	Resolution
13696296	The connector dataset name should be customizable.	This issue has been resolved. You need to customize the CLIST.DONE.FILE dataset name in order to get the Oracle Identity Manager Top Secret Advanced connector up and running.
13828279	The user is generating an exception crash during reconciliation.	This issue has been resolved. The user can now successfully run the reconciliation.
13847821	The RWAIT parameter is not being honored by the pioneer agent before sending to LDAP.	This issue has been resolved. The RWAIT parameter is now successfully honored by the pioneer agent before sending to LDAP.

Software Updates in Release 9.0.4.14

The following are the software updates in release 9.0.4.14:

- Support for New Lookup Definition Scheduled Tasks
- Support for Provisioning Functions
- Support for New IT Resource Parameters
- Support for SSL Configuration in LDAP Gateway
- Support for Voyager and Pioneer Parameters Using a Control File
- Support for Voyager and Pioneer Enhanced Operator Command

- Support for Post-processing within Pioneer Based on Top-Secret Command
- Support for ALIAS Processing within Pioneer Based on LDAP Command
- Support for New Scheduled Tasks Configuration
- Support for Initial Reconciliation Through Scheduled Task

Support for New Lookup Definition Scheduled Tasks

From this release onward, the connector includes scheduled tasks for storing all resources, profiles, facilities, and datasets in lookup definitions. These lookups are used during the provisioning process, allowing the user to select an existing profile, resource, facility, or dataset from a lookup list, instead of manually entering the name in the provisioning form.

See Section 1.5, "Connector Objects Used During Reconciliation and Provisioning" for more information.

Support for Provisioning Functions

From this release onward, new provisioning functions are supported by the connector.

See Section 1.5.2, "Supported Functions for Provisioning" for more details.

Support for New IT Resource Parameters

From this release onward, new IT resource parameters are supported by the connector.

See Section 2.3, "Configuring the IT Resource" for more information.

Support for SSL Configuration in LDAP Gateway

From this release onward, SSL configuration in LDAP Gateway has been supported.

SeeSection 2.6, "Installing and Configuring the LDAP Gateway" for more information.

Support for Voyager and Pioneer Parameters Using a Control File

From this release onward, the Voyager STC will not pass any STC parameters. They are now contained in a QSAM file pointed to by the PARMFLE "DD" statement. Pioneer will now only pass four parameters, TCPN, IPAD, PORT, and DEBUG. All other parameters are passed through the control file.

Support for Voyager and Pioneer Enhanced Operator Command

In this release, new set of commands for Pioneer and Voyager are included.

See Chapter 3, "Connector Deployment on the Mainframe" for more information.

Support for Post-processing within Pioneer Based on Top-Secret Command

In this release, ability for Pioneer to post-process with the usage of one of the three Top-Secret commands, Create, Addto, and Remove commands, has been introduced. The format and functionally is explained in Chapter 3, "Connector Deployment on the Mainframe". The output of the Post-Processing, where it worked or not, is the responsibility of the installation and not Pioneer.

Support for ALIAS Processing within Pioneer Based on LDAP Command

In this release, ability for Pioneer process LDAP ALIAS Defines and Deletes, has been introduced. The ALIAS request will come into Pioneer and Pioneer using the INJCLR "DD" submits the DEFINE or DELETE with the INJCLR JCl wrapped around it. The output is sent back to the LDAP. The "JWAIT= parameter" is new and is used as a wait timer for the job to finish completion.

See Section 3.8, "Configuring the Started Tasks" for more information.

Support for New Scheduled Tasks Configuration

From this release onward, a set of new scheduled task configurations have been supported.

See Table 4.2, "Scheduled Tasks for Lookup Field Synchronization" for more information.

Support for Initial Reconciliation Through Scheduled Task

From this release onward, initial reconciliation is no longer performed using the topsecret-initial-recon-adapter deployment. Instead, initial reconciliation is supported through the TopSecret Reconcile All Users scheduled task.

See Section 5.4, "Removing Attributes Mapped for Target Resource Reconciliation" for more details.

Resolved Issues in Release 9.0.4.14

The following table lists issues resolved in release 9.0.4.14:

Bug Number	Issue	Resolution
12977414	No support for expiration dates when modifying a user (TSS ADDTO)	This issue has been resolved. All ADDTO attributes, including FIRST, AFTER, and BEFORE, are now supported.

Software Updates in Release 9.0.4.13

The following are the software updates in release 9.0.4.13:

- Support for New Oracle Identity Manager Release
- Support for Request-Based Provisioning
- Resolved Issues in Release 9.0.4.13

Support for New Oracle Identity Manager Release

From this release onward, the connector can be installed and used on Oracle Identity Manager 11*g* release 1 (11.1.1). Where applicable, instructions specific to this Oracle Identity Manager release have been added in the guide.

See Section 1.1, "Certified Components" for the full list of certified Oracle Identity Manager releases.

Support for Request-Based Provisioning

From this release onward, the connector provides support for request-based provisioning on Oracle Identity Manager 11*g* release 1 (11.1.1).

See Section 4.7.2, "Request-Based Provisioning" for more information.

Resolved Issues in Release 9.0.4.13

The following table lists issues resolved in release 9.0.4.13:

Bug Number	Issue	Resolution
6361887	The Out of Disk Space error was not handled correctly.	This issue has been resolved. The Out of Disk Space error is now handled correctly.

Bug Number	Issue	Resolution
9704749	The maclib.xmi file was missing from the Mainframe_TS.zip file on the installation media.	This issue has been resolved. The maclib.xmi file is now bundled in the Mainframe_TS.zip file on the installation media.
9735838	During reconciliation, CPU utilization by the LDAP Gateway reached very high levels.	This issue has been resolved. CPU utilization by the LDAP Gateway now remains within acceptable levels.

Software Updates in Release 9.0.4.12

The following are software updates in release 9.0.4.12:

- With the DEBUG log level, the connector can now record log messages that describe issues related to storing of user records in the internal meta-store. See Section 1.3.2, "Connector Operations" for information about the internal meta-store.
- The connector can recognize and prevent the recording of invalid encrypted messages in the log files.

Software Updates in Release 9.0.4.11

The following are software updates in release 9.0.4.11:

Support for the SOURCE Multivalued Attribute

From this release onward, the connector supports the SOURCE multivalued attribute for reconciliation and provisioning operations. See Section 1.5.6, "SOURCE Attributes for Provisioning" for information about attribute mappings for this multivalued attribute.

Software Updates in Release 9.0.4.7

The following are software updates in release 9.0.4.7:

Software Updates in Release 9.0.4.6

The following are software updates in release 9.0.4.6:

- Support for the Suspend Until Function
- Resolved Issues in Release 9.0.4.6

Support for the Suspend Until Function

The connector now supports provisioning operations corresponding to the following target system functions:

- TSS ADD(acid) ASUSPEND UNTIL(*DATE*): An administrative user suspends a user either indefinitely (no date is entered) or up to a specified date.
- TSS REMOVE(acid) ASUSPEND UNTIL(): An administrative user unsuspends a user.
- TSS ADD(acid) SUSPEND UNTIL(*DATE*): A user suspends another user either indefinitely (no date is entered) or up to a specified date.
- TSS REMOVE(acid) SUSPEND UNTIL(): A user unsuspends another user.

> **Note:** For a Suspend operation, you cannot specify the current date. The date specified must be either the next day or a future date.

Resolved Issues in Release 9.0.4.6

The following are issues resolved in release 9.0.4.6:

Bug Number	Issue	Resolution
8582428	During provisioning operations, assignment of a group to a user failed.	This issue was resolved in release 9.0.4.5. Group assignment to a user does not fail during provisioning operations.
8909417	The connector allows you to create and use multiple resource objects to represent multiple user types in your organization. This is described in the "Configuring Limited Reconciliation" section of the connector guide. In earlier releases, changes to the Enabled/Disabled/Revoked status of users on the target system were not reconciled if you used multiple resource objects.	This issue has been resolved. Changes in user status are reconciled into Oracle Identity Manager even when you configure multiple resource objects.

Software Updates in Release 9.0.4.5

The following are issues resolved in release 9.0.4.5:

Bug Number	Issue	Resolution
8715777	During a reconciliation run, a parsing error was encountered if there was no data between the PROFILES and INSTDATA segments fetched from the target system.	This issue has been resolved. Data is always present between the PROFILES and INSTDATA segments during a reconciliation run.

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.

Software Updates in Release 9.0.4.3

The following are issues resolved 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 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, group, 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 2-14.
- Information about reconciliation based on user status has been added in "Configuring Account Status Reconciliation" on page 4-7.
- Steps to add a new field for provisioning have been added in "Adding New Fields for Provisioning" on page 4-5.
- Known issues related to the following bugs have been added in Chapter 7, "Known Issues and Workarounds":
  - 6668844
  - 6904041
  - 7033009
- Information about integrating the Reconciliation Agent exit with existing Top Secret exits has been added in "Installing or Integrating the Reconciliation Agent Exit" on page 3-9.

Documentation-Specific Updates

The following sections discuss documentation-specific updates:

- Documentation-Specific Updates in Release 9.0.4.20
- Documentation-Specific Updates in Release 9.0.4.19
- Documentation-Specific Updates in Release 9.0.4.18
- Documentation-Specific Updates in Release 9.0.4.17
- Documentation-Specific Updates in Release 9.0.4.16
- Documentation-Specific Updates in Release 9.0.4.15
- Documentation-Specific Updates in Release 9.0.4.14
- Documentation-Specific Updates in Release 9.0.4.13

- Documentation-Specific Updates in Release 9.0.4.2 Through 9.0.4.12

Documentation-Specific Updates in Release 9.0.4.20

The following documentation-specific updates have been made in revision "23" of release 9.0.4.20:

- References pertaining to topsecret-agent-recon, VOYAGER_ID.properties, RECOVERY_INTERVAL, and DNS-RECOVERY_INTERVAL have been removed throughout the document as they are no longer used.
- The "omvsoefilep" entry in the LDAP Gateway Name column of Table 1–5, " Unmapped User Attributes for Target Resource Reconciliation and Provisioning" has been updated.
- A "Note" on obtaining TSSINSTX exit source code through Oracle Support has been removed from Section 3.2, "Deploying the Reconciliation Agent and Provisioning Agent" as it is no longer supported.
- Table 3–13, " Voyager Control File Parameters" has been modified as follows:
  - The "CONNECT-MSGS" parameter has been changed to "CONNECT_MSGS."
  - The "CONNECT_INTV=nn" and "CONNECT_RETRY=nnn" parameters have been added.
- Description of the "CACHE_DELAY=" parameter has been modified in Table 3–13, " Voyager Control File Parameters".

The following documentation-specific updates have been made in revision "22" of release 9.0.4.20:

- Updates to Appendix F, "LOADDSN Member and the File Contents" section.
- Updates to Appendix G, "Reconciliation Agent (Voyager) Messages" section
- Updates to Appendix H, "Provisioning Agent (Pioneer) Messages" section
- Updates to Appendix J, "Pioneer and Voyager LONG_FDTNAME=Y Processing" section

The following documentation-specific updates have been made in revision "21" of release 9.0.4.20:

- The following rows have been added:
  - Row "rexxlib.xmi" to Table 3–1, " JES2 XMIT Files".
  - Row "rexxlib.xmi" to Table 3–2, " File name on the Client Machine and on the Mainframe Host".
  - Row "REXXLIB.XMIT" to Table 3–3, " XMIT File Names and PDS Names".
  - Rows "IEBCPYRX" and "REXXCL" to Table 3–4, " JCLLIB members and their description".
  - Row "IOException:" to Table 6–1, " Troubleshooting Tips".
- The following information has been added:
  - Table 1–3, " Attribute Characteristics"
  - Section 1.3.2.2, "CFILE Reconciliation Process"
  - Appendix J, "Pioneer and Voyager LONG_FDTNAME=Y Processing"
  - Appendix K, "Mainframe Language Environment Runtime Options"

- The following information has been modified:
  - The "Oracle Identity Manager" row of Table 1–1, " Certified Components".
  - Section 1.3.2.1, "Full Reconciliation Process"
  - Section 1.4.1, "Target Resource Reconciliation"
  - Table 1–5, " Unmapped User Attributes for Target Resource Reconciliation and Provisioning"
  - Section 1.5.3, "User Attributes for Target Resource Reconciliation and Provisioning"
  - Section 3.2, "Deploying the Reconciliation Agent and Provisioning Agent"
  - Section 3.6, "Creating a CA Top Secret Account for Connector Operations"
  - Table 3–12, " Pioneer Control File Parameters"
  - Table 3–13, " Voyager Control File Parameters"
  - Section 5.8, "Configuring Windows Service"
  - Chapter 7, "Known Issues and Workarounds"
  - Rows "PSAMPLE" and "VSAMPLE" of Table F–1, " Steps of LOADDSN Member and File Contents".
  - Appendix G, "Reconciliation Agent (Voyager) Messages"
- Removed references to trusted source reconciliation. Trusted source reconciliation is no longer supported.

Documentation-Specific Updates in Release 9.0.4.19

The following documentation-specific updates have been made in revision "20" of release 9.0.4.19:

- In Table 2–6, " Properties in the tops.properties File" rows for configDNames and configAttrs have been updated for latest information.
- Section 5.3, "Adding Custom Fields for Provisioning" has been updated for latest information.
- Section 5.7, "Initial LDAP Gateway Population and Full Reconciliation" has been updated for latest information.
- In Table 6–1, " Troubleshooting Tips" an additional entry has been added.
- In Appendix C, "Top Secret CFILE -> LDAP Attribute Mapping" a note on user's profiles and facilities child data has been added.

The following documentation-specific updates have been made in revision "19" of release 9.0.4.19:

- In Table 1–1, " Certified Components" a note on prerequisites for the connector has been added.
- Table 1–4, " Mapped User Attributes for Target Resource Reconciliation and Provisioning" has been updated.
- Table 1–5, " Unmapped User Attributes for Target Resource Reconciliation and Provisioning" has been updated.
- Section 5.1.2, "Adding Custom Fields to Oracle Identity Manager" has been updated.

- Section 5.3, "Adding Custom Fields for Provisioning" has been updated.
- Table C–1, " CFILE LDAP Attribute Mapping" has been updated.

The following documentation-specific updates have been made in revision "18" of release 9.0.4.19:

- In Table 1–1, " Certified Components" the "Oracle Identity Manager" row has been modified, and the "LDAP Gateway requirements" row has been added.
- Table 1–5, " Unmapped User Attributes for Target Resource Reconciliation and Provisioning" has been added for the information on unmapped user attributes for Target Resource Reconciliation and Provisioning.
- In Section 1.4.4, "High Availability Feature of the Connector" a note has been added on shutdown for scenario 2 and scenario 3.
- Section 1.5.4, "PROFILE Attributes for Target Resource Reconciliation and Provisioning" has been modified.
- Section 1.5.5, "GROUP Attributes for Target Resource Reconciliation and Provisioning" has been modified.
- Section 1.5.6, "SOURCE Attributes for Provisioning" has been modified.
- Section 1.5.7, "FACILITY Attributes for Target Resource Reconciliation and Provisioning" has been modified.
- Table 2–1, " Files and Directories That Comprise the Connector" been updated with latest information on files and directories.
- Table 2–6, " Properties in the tops.properties File" has been updated for new properties.
- Section 3.1, "Reviewing Deployment Requirements" and Section 3.2, "Deploying the Reconciliation Agent and Provisioning Agent" have been updated for latest information.
- Section "Before Running the Connector Installer" has been removed from the guide as it is no longer required.
- Table 3–4, " JCLLIB members and their description" has been updated for new member names.
- Table 3–6, " Voyager DDs and their corresponding CREATDSN DD entries" has been updated for CACHESAV row.
- Section 3.8, "Configuring the Started Tasks" has been modified for the latest information.
- Section 3.10, "Starting Up and Shutting Down the Reconciliation Agent" has been updated for latest information.
- In Table 3–11, " CREATEXP (Optional CFILE) Variables and Values" CREATEXP (Optional CFILE) variables and values have been added with steps.
- Table 3–12, " Pioneer Control File Parameters" has been updated with new parameters.
- MSGID01 usage is documented in Table 3–13, " Voyager Control File Parameters".
- PIONEER and VOYAGER Operator Commands F PIONEER,JWAIT=999 row has been removed from Table 3–14, " Pioneer and Voyager Operator Commands".
- Section 5.8, "Configuring Windows Service" has been added to include Windows Service instructions in the doc.

- Appendix A, "Authorized Libraries" has been updated for latest information.
- Appendix B, "AES 128 User Key Definition and Usage" has been added.
- Appendix D, "Top-Secret CFILE Processing" has been updated for latest information.
- Appendix F, "LOADDSN Member and the File Contents" has been updated for latest information.
- Appendix I, "Pioneer Searches – Initiated from the LDAP" has been added.
- The information related to trusted reconciliation has been removed from the entire guide as it is not supported.

Documentation-Specific Updates in Release 9.0.4.18

The following are the documentation-specific updates in this release:

- Table 1–1 has been updated for certified components.
- Section 1.3.2.4, "Provisioning Process" has been updated for provisioning process.
- Section 1.5.3, "User Attributes for Target Resource Reconciliation and Provisioning" has been updated for user attributes.
- Section 1.5.4, "PROFILE Attributes for Target Resource Reconciliation and Provisioning" has been updated for profile provisioning operations.
- Section 1.5.5, "GROUP Attributes for Target Resource Reconciliation and Provisioning" has been added for group provisioning operations.
- Section 1.5.6, "SOURCE Attributes for Provisioning" has been updated for source provisioning operations.
- Section 1.5.7, "FACILITY Attributes for Target Resource Reconciliation and Provisioning" has been updated for facility provisioning operations.
- Section 1.5.8, "DATASET Attributes for Provisioning" has been updated for dataset provisioning operations.
- Section 2.1, "Files and Directories That Comprise the Connector" has been updated for latest files and directories.
- Section 3.7, "Summary of the Deployment Procedure" has been updated for procedure to deploy the connector components on the target system.
- In Section 3.1, "Reviewing Deployment Requirements," a note on APF Authorization has been updated.
- Section 3.2, "Deploying the Reconciliation Agent and Provisioning Agent" has been updated for reconciliation agent and provisioning agent process.
- Section 3.3, "Editing the Mainframe Batch Job Files" has been updated for information on editing the mainframe batch job files.
- Section 3.8, "Configuring the Started Tasks" has been updated for started tasks.
- Section 4.2, "Scheduled Tasks for Lookup Field Synchronization" has been added for the scheduled tasks for lookup field synchronization.
- Section 4.4, "Configuring Reconciliation" has been added for configuring reconciliation.
- Section 5.2, "Adding Custom Multivalued Fields for Reconciliation" has been added for information on custom multivalued fields for reconciliation.

- Section 5.3, "Adding Custom Fields for Provisioning" has been updated for additional attributes for provisioning.
- Section 5.7, "Initial LDAP Gateway Population and Full Reconciliation" has been added for the information on initial LDAP gateway population and full reconciliation.
- Appendix G, "Reconciliation Agent (Voyager) Messages" has been updated for new messages.
- Appendix C, "Top Secret CFILE -> LDAP Attribute Mapping" has been added.
- Instructions specific to Oracle Identity Manager release 11.1.2.*x* have been added in the following sections:
  - Section 2.2, "Running the Connector Installer"
  - Section 2.3, "Configuring the IT Resource"
  - Section 2.4, "Configuring Oracle Identity Manager"
  - Section 2.6, "Installing and Configuring the LDAP Gateway"
  - Section 4.3, "Configuring the Sources Lookup Field"
  - Section 4.6, "Configuring Scheduled Tasks"
  - Section 4.8, "Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later"
  - Section 5.1, "Adding Custom Fields for Target Resource Reconciliation"

Documentation-Specific Updates in Release 9.0.4.17

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.16

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.15

The following is the documentation-specific update in this release:

- In Section 3.10, "Starting Up and Shutting Down the Reconciliation Agent", a note on Voyager Agent has been updated for Pioneer Agent and Startup procedure.

Documentation-Specific Updates in Release 9.0.4.14

The following are the documentation-specific updates in this release.

- In Table 1–4, " Mapped User Attributes for Target Resource Reconciliation and Provisioning", changes have been made in the user attributes.
- A note has been added on the number of characters allowed in the text field for the SingleValueAttributes. See Table 4–3, " Attributes of the Top Secret Reconcile All Users Scheduled Task" for more information.
- In the entire document, the name of the scheduled task, "TSS Reconcile All Users scheduled task" has been changed to "TopSecret Reconcile All Users scheduled task".

Documentation-Specific Updates in Release 9.0.4.13

There are no documentation-specific updates in this release.

Documentation-Specific Updates in Release 9.0.4.2 Through 9.0.4.12

The following sections discuss documentation-specific updates have been made in releases 9.0.4.2 to 9.0.4.12:

- The user attribute 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 7, "Known Issues and Workarounds" have been moved to "Guidelines on Using the Connector" on page 6-2.
- Information about enabling logging on the LDAP Gateway server has been added in "Installing and Configuring the LDAP Gateway" on page 2-17.
- 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 the TCP/IP Connection and Started Tasks
- In the "Certified Languages" section, Arabic has been added to the list of languages that the connector supports.
- In Table 1–1, " Certified Components", changes have been made in the Target Systems row. Information about certified deployment configurations has been removed from "Reviewing Deployment Requirements" on page 3-1.
- Major changes have been made in the structure of the guide. In addition, in Section 1.1, "Certified Components," CA Top Secret r14 has been added to the list of certified target systems.
- In Table 1–1, " Certified Components", the minimum Oracle Identity Manager release has been changed to 9.1.0.1 and the JDK requirement of release 1.5 or later has been added.
- Section 5.6, "Configuring the Generation of Single-Use Passwords for the Reset Password Operation" has been added.

1 About the Connector

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications. This guide discusses the connector that enables you to use CA Top Secret as a managed (target) resource of identity data for Oracle Identity Manager.

The advanced connector for CA Top Secret provides a native interface between CA Top Secret installed on an IBM z/OS mainframe and Oracle Identity Manager. The connector functions as a trusted virtual administrator on the target system, performing tasks related to creating and managing users.

In the account management (target resource) mode of the connector, information about users (ACIDs) created or modified directly on the target system can be reconciled into Oracle Identity Manager. In addition, you can use Oracle Identity Manager to perform provisioning operations on the target system.

Users on CA Top Secret correspond to accounts or resources assigned to OIM Users.

This chapter contains the following topics:

- Section 1.1, "Certified Components"
- Section 1.2, "Certified Languages"
- Section 1.3, "Connector Architecture"
- Section 1.4, "Features of the Connector"
- Section 1.5, "Connector Objects Used During Reconciliation and Provisioning"

1.1 Certified Components

Table 1–1 lists the certified components.

Table 1–1 Certified Components

Item	Requirement
Oracle Identity Manager	You can use one of the following releases of Oracle Identity Manager: ■ Oracle Identity Manager 11*g* release 2 (11.1.2.0.1) and any later BP in this release track **Note:** In this guide, **Oracle Identity Manager release 11.1.2.*x*** has been used to denote Oracle Identity Manager 11*g* release 2 (11.1.2.0.1) or any later BP in this release track in the 11.1.2.*x* series that the connector supports. ■ Oracle Identity Manager 11*g* release 2 PS1 (11.1.2.1.0) and any later BP in this release track ■ Oracle Identity Manager 11*g* release 2 PS2 (11.1.2.2.0) and any later BP in this release track **Note:** Prerequisites for this connector to work with 11.1.2.2.0 are: ARU 17421629. ADF patch ARU 17714568. SP procedure for Recon ■ Oracle Identity Manager 11*g* release 2 PS3 (11.1.2.3.0)
JDK	The JDK version can be one of the following: ■ For Oracle Identity Manager release 11.1.1.*x*, use JDK 1.6 update 18 or later. ■ For Oracle Identity Manager release 11.1.2.*x* or later, use JDK 1.6 update 31 or later.
Target Systems	CA Top Secret r8, r9, r12, or r14
Infrastructure Requirements: Message transport layer between the Oracle Identity Manager and the mainframe environment	TCP/IP with Advanced Encryption Standard (AES) encryption
Target system user account for reconciliation and provisioning operations	IBM Authorized Program Facility (APF) authorized account with System Administrators privileges See Section 3.6, "Creating a CA Top Secret Account for Connector Operations" for more information about this account.
Pioneer and Voyager	Pioneer and Voyager are written in single thread LE Cobol. They were developed to run above the 16M line. Options that can adversely affect these STCs are LE run options: ALL31(OFF) instead of ON STACK(,,,BELOW,,) instead of STACK(,,,ANYWHERE,,)
LDAP Gateway	■ Operating system: Microsoft Windows, or Linux, any flavor except AIX ■ JDK 1.7 or above

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

> **See Also:** *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about supported special characters supported by Oracle Identity Manager

1.3 Connector Architecture

This section contains the following topics:

- Section 1.3.1, "Connector Components"
- Section 1.3.2, "Connector Operations"

1.3.1 Connector Components

The CA Top Secret Advanced connector contains the following components:

- **LDAP Gateway**: The LDAP Gateway receives instructions from Oracle Identity Manager in the same way as any LDAP version 3 identity store. These LDAP commands are then converted into native commands for CA Top Secret and sent to the Provisioning Agent. The response, which is also native to CA Top Secret, is parsed into an LDAP-format response and returned to Oracle Identity Manager.

  During reconciliation, the LDAP Gateway receives event notification, converts the events to LDAP format, and then forwards them to Oracle Identity Manager, or events can be stored in the LDAP Gateway internal store and pulled into Oracle Identity Manager by a scheduled task.

- **Provisioning Agent (Pioneer)**: The Pioneer Provisioning Agent is a mainframe component. It receives native mainframe CA Top Secret identity and authorization change events from the LDAP Gateway. These events are processed against the CA Top Secret authentication repository, in which all provisioning updates from the LDAP Gateway are stored. The response is parsed and returned to the LDAP Gateway.

  > **Note:** At some places in this guide, the Provisioning Agent is referred to as **Pioneer.**

- **Reconciliation Agent (Voyager):** The Reconciliation Agent captures mainframe events by using a Top Secret exit, which is a program run after events in CA Top Secret are processed. These events include the ones generated at TSO logins, the command prompt, batch jobs, and other native events. These events are stored in the subpool cache area that is established by a supplied, standard z/OS procedure

(STARTUP). The Reconciliation Agent captures these events, transforms them into LDAPv3 protocol notification messages, and then sends them to Oracle Identity Manager through the LDAP Gateway.

> **Note:** At some places in this guide, the Reconciliation Agent is referred to as **Voyager.**

- **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 is used for the transport of messages.

  TCP/IP with Advanced Encryption Standard (AES) encryption using 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.

1.3.2 Connector Operations

This section provides an overview of the following processes:

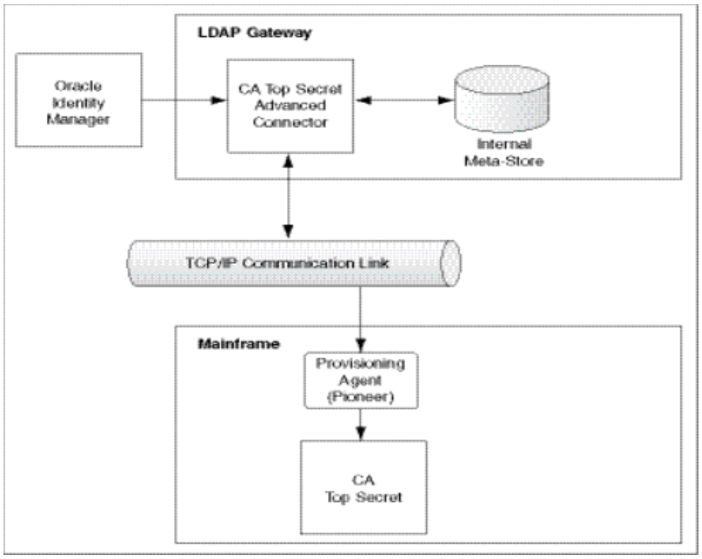
- Section 1.3.2.1, "Full Reconciliation Process"
- Section 1.3.2.2, "CFILE Reconciliation Process"
- Section 1.3.2.3, "Incremental (Real-Time) Reconciliation Process"
- Section 1.3.2.4, "Provisioning Process"

1.3.2.1 Full Reconciliation Process

Full reconciliation involves fetching existing user data from the mainframe to Oracle Identity Manager. This user data is converted into accounts or resources for OIM Users.

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

Figure 1–1 Full Reconciliation Process


LDAP Gateway
Oracle Identity Manager
CA Top Secret Advanced Connector
Internal Meta-Store
TCP/IP Communication Link
Mainframe
Provisioning Agent (Pioneer)
CA Top Secret

The following is a summary of the full reconciliation process:

Note: The detailed procedure is explained later in this guide.

1. Set values for the properties defined in the TSS Reconcile All Users scheduled task.
2. Run the scheduled task. The task sends a search request to the LDAP Gateway.
3. The LDAP Gateway encrypts the search request and then sends it to the Provisioning Agent on the mainframe.
4. The Provisioning Agent encrypts user profile data received from CA Top Secret and then passes this data to the LDAP Gateway.
5. The LDAP Gateway decrypts the user profile data. If the user profile data does not include any changes when compared to the OIM user's existing resource data, then the event is ignored and reconciliation continues with the next user on the target system. If the user profile data includes a change, then the LDAP Gateway passes the data on to Oracle Identity Manager.
6. This user profile data is converted into accounts or resources for OIM Users.

1.3.2.2 CFILE Reconciliation Process

CFILE reconciliation involves fetching existing user data in the form of a TSSCFILE extract from the mainframe to Oracle Identity Manager. This user data is converted into accounts or resources for OIM Users.

The following is a summary of the CFILE reconciliation process:

Note: The detailed procedure is explained later in this guide.

1. Generate an extract file of user data by executing the TSSCFILE command on the CA Top Secret system.
2. Convert the CFILE data into XML format by running the Conv2XML process on the CA Top Secret system. The XML is stored in a dataset.
3. Set values for the properties defined in the TSS Reconcile Users to Internal LDAP scheduled task.
4. Run the scheduled task. The task sends a request to the LDAP gateway to retrieve the XML file from Pioneer.
5. The Provisioning Agent receives the request from LDAP Gateway and reads the data from the XML dataset.
6. The Provisioning Agent encrypts the user data and passes it to the LDAP Gateway.
7. The LDAP Gateway decrypts the user profile data. The data is stored in the LDAP Gateway's internal data-store.
8. Set values for the properties defined in the TSS Reconcile LDAP Users to OIM scheduled task.
9. Run the scheduled task. The next step depends on the setting in the IT resource as mentioned below:
   a. If you set the "Last Modified Time Stamp" property to zero (0), then all user profile data will be retrieved from the LDAP internal store.

b. If you configure "Last Modified Time Stamp" property with a timestamp, then only user profile data updated since the timestamp will be retrieved from the LDAP internal store.

10. The next step depends on the user data as mentioned below:

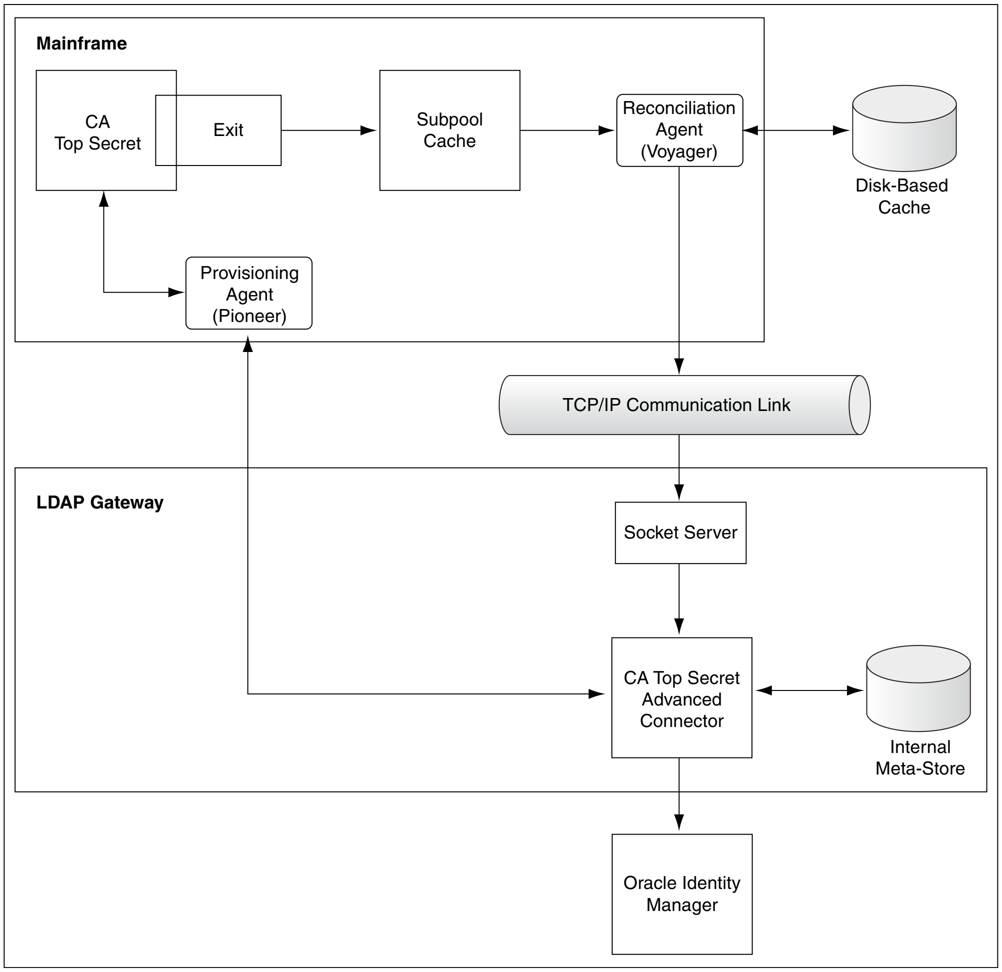
    a. If the user profile data does not include any changes when compared to the OIM user's existing resource data, then the event is ignored and reconciliation continues with the next retrieved user.

    b. If the user profile data includes a change, then the LDAP Gateway passes the data on to Oracle Identity Manager. The user profile data is converted into accounts or resources for OIM Users.

1.3.2.3 Incremental (Real-Time) Reconciliation Process

Incremental or real-time reconciliation is initiated by the exit that works in conjunction with the Reconciliation Agent. Figure 1–2 shows the flow of data during this form of reconciliation.

Figure 1–2 Reconciliation Process



The following is a summary of the reconciliation process:

1. Incremental reconciliation begins when a user is created or, updated on CA Top Secret. This event might take place either directly on the mainframe or in response to a provisioning operation on Oracle Identity Manager.
2. TSSINSTX is a standard CA Top Secret exit. This exit is used in conjunction with the Reconciliation Agent. The exit detects the event and sends a message containing user data to Subpool 231 (cache).
3. The Reconciliation Agent polls Subpool 231. When it finds the message in the subpool, it reads the message into its buffer. This frees up the subpool.
4. The Reconciliation Agent opens up a connection with the LDAP Gateway, and then sends the message to the gateway over TCP/IP.

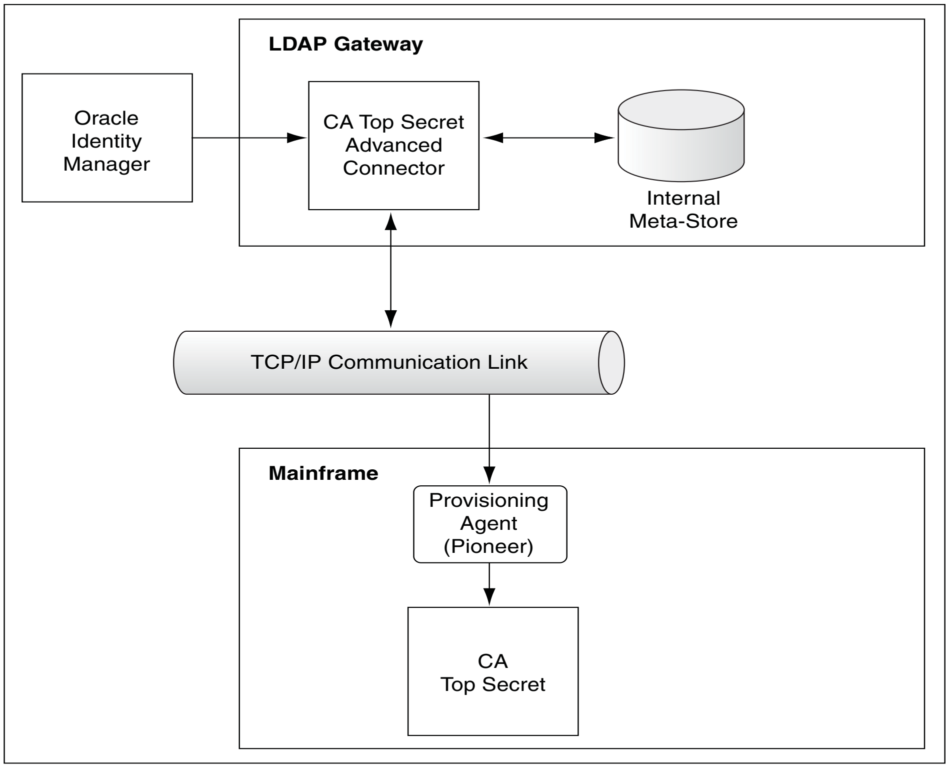
   > **Note:** Messages sent to the LDAP Gateway are encrypted using AES-128 encryption.

5. The LDAP Gateway decrypts the user profile data. If the user profile data does not include any changes when compared to the OIM user's existing resource data, then the event is ignored and reconciliation continues with the next user on the target system. If the user profile data includes a change, then the LDAP Gateway can store the data internally for use by a scheduled task, or it can pass the data on to Oracle Identity Manager.
6. Oracle Identity Manager processes the message and creates or updates either the corresponding CA Top Secret resource or the OIM User.

1.3.2.4 Provisioning Process

Figure 1–3 shows the flow of data during provisioning.

Figure 1–3 Provisioning Process


LDAP Gateway
Oracle Identity Manager
CA Top Secret Advanced Connector
Internal Meta-Store
TCP/IP Communication Link
Mainframe
Provisioning Agent (Pioneer)
CA Top Secret

The following is a summary of the provisioning process:

1. Provisioning data submitted from the Oracle Identity System Administration is sent to the LDAP Gateway.
2. The LDAP Gateway converts the provisioning data into mainframe commands, encrypts the commands, and converts the message from ASCII to EBCDIC.
3. The Provisioning Agent executes the commands and runs them on the mainframe and within the Pioneer STC (Started Task) using the RACF API (IRRSEQ00).
4. The Provisioning Agent converts the RACF API output to ASCII and encrypts the message prior to sending it back to the LDAP Gateway.
5. The outcome of the operation on the mainframe is displayed on the Oracle Identity Manager console. A more detailed message is recorded in the connector log file.

1.4 Features of the Connector

The following are features of the connector:

- Section 1.4.1, "Target Resource Reconciliation"
- Section 1.4.2, "Full and Incremental Reconciliation"
- Section 1.4.3, "Encrypted Communication Between the Target System and Oracle Identity Manager"
- Section 1.4.4, "High Availability Feature of the Connector"

1.4.1 Target Resource Reconciliation

You can use the connector to configure CA Top Secret as a target resource of Oracle Identity Manager.

1.4.2 Full and Incremental Reconciliation

After you deploy the connector, you can perform full reconciliation to bring all existing user data from the target system to Oracle Identity Manager. After the first full reconciliation run, change-based or incremental reconciliation is automatically enabled and active. Incremental reconciliation is a real-time process. User changes on the target system are directly sent to Oracle Identity Manager or stored in the LDAP Gateway internal store.

You can perform a full reconciliation run at any time. See Section 4.4.1, "Full Reconciliation" for more information.

1.4.3 Encrypted Communication Between the Target System and Oracle Identity Manager

AES-128 encryption is used to encrypt data that is exchanged between the LDAP Gateway and the Reconciliation Agent and Provisioning Agent on the mainframe.

1.4.4 High Availability Feature of the Connector

The following are component-failure scenarios and the response of the connector to each scenario:

- **Scenario 1: The Reconciliation Agent is running and the LDAP Gateway stops responding**

  1. The Reconciliation Agent stops sending messages (event data) to the LDAP Gateway.
  2. Messages that are not sent are stored in the subpool cache.
  3. When the LDAP Gateway is brought back online, the Reconciliation Agent reads data from the subpool cache and then sends messages to the LDAP Gateway.

- **Scenario 2: The LDAP Gateway is running and the Reconciliation Agent stops responding**

  1. Event data is sent to the subpool cache.
  2. When the Reconciliation Agent is brought back online, it reads data from the subpool cache and then sends messages to the LDAP Gateway.

  Note: During SHUTDOWN, there is a possibility that events that had been sent to the LDAP might be saved and re-sent again once the Agent is brought back online. This is to ensure no data lose and this process will re-list the event data to provide the most current view.

- **Scenario 3: The LDAP Gateway is running and the mainframe stops responding**

  1. Messages that are in the subpool cache are written to disk.
  2. When the mainframe is brought back online, event data written to disk is again stored in the subpool cache.

3. The Reconciliation Agent reads data from the subpool cache and then sends messages to the LDAP Gateway.

> **Note:** During SHUTDOWN, there is a possibility that events that had been sent to the LDAP might be saved and re-sent again once the Agent is brought back online. This is to ensure no data lose and this process will re-list the event data to provide the most current view.

- **Scenario 4: The LDAP Gateway is running and the Provisioning Agent or mainframe stops responding**

  The process task that sends provisioning data to the LDAP Gateway retries the task.

- **Scenario 5: The subpool is stopped by an administrator**

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

1.5 Connector Objects Used During Reconciliation and Provisioning

The following sections provide information about connector objects used during reconciliation and provisioning:

- Section 1.5.1, "Supported Functions for Target Resource Reconciliation"
- Section 1.5.2, "Supported Functions for Provisioning"
- Section 1.5.3, "User Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.5.4, "PROFILE Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.5.5, "GROUP Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.5.6, "SOURCE Attributes for Provisioning"
- Section 1.5.7, "FACILITY Attributes for Target Resource Reconciliation and Provisioning"
- Section 1.5.8, "DATASET Attributes for Provisioning"
- Section 1.5.9, "Provisioning GENCERT Operations"
- Section 1.5.10, "Provisioning GENREQ Operations"
- Section 1.5.11, "Reconciliation Rule"
- Section 1.5.12, "Reconciliation Action Rules"

1.5.1 Supported Functions for Target Resource Reconciliation

The connector supports reconciliation of user data from the following events:

- Create user
- Modify user
- Rename user

- Change password
- Reset password
- Suspend user
- Suspend user until
- Delete user
- Unsuspend user
- Unsuspend user until

1.5.2 Supported Functions for Provisioning

Table 1–2 lists the provisioning functions supported by the connector.

Table 1–2 Supported Functions for Provisioning

Function	Description	Mainframe Command
Create user	Adds new users on CA Top Secret	TSS CREATE
Modify user	Modifies user information on CA Top Secret	TSS REPLACE
Rename user	Modifies user's UID on CA Top Secret	TSS RENAME
Change password	Changes user passwords on CA Top Secret in response to password changes made on Oracle Identity Manager through user self-service	TSS REPLACE
Reset password	Resets user passwords on CA Top Secret The passwords are reset by the administrator.	TSS REPLACE
Suspend user	Disables users on CA Top Secret	TSS ADDTO
Suspend user until	Disables users up to the specified date on CA Top Secret	TSS ADDTO
Unsuspend user	Enables users on CA Top Secret	TSS REMOVE
Delete users	Removes users from CA Top Secret	TSS DELETE
Grant user access to data sets	Adds users to data set and assigns the specified access rights	TSS PERMIT
Grant user access to privileges (TSO)	Provides TSO login access to users	TSS REPLACE
Removes user access to data sets	Removes users from data sets	TSS REVOKE
Grant user access to facilities	Adds users to facilities and assigns the specified access rights	TSS ADDTO
Removes user access to facilities	Removes users from facilities	TSS REMOVE
Grant user access to groups	Adds users to groups	TSS ADDTO
Remove user access to groups	Removes users from groups	TSS REMOVE
Grant user access to profiles	Add users to profiles	TSS ADDTO
Remove user access to profiles	Removes users from profiles	TSS REMOVE

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

Function	Description	Mainframe Command
Grant user access to sources	Adds users to sources	TSS ADDTO
Remove user access to sources	Removes users from sources	TSS REMOVE
Generate certificate	Generates a digital certificate associated with the user	TSS GENCERT
Generate certificate request	Generates a PKCS#10 base64-encoded digital certificate request and writes it to a data set	TSS GENREQ

1.5.3 User Attributes for Target Resource Reconciliation and Provisioning

The CA Top Secret connector uses three categories of attributes: mapped, unmapped, and custom.

Mapped and unmapped attributes are supported in the LDAP Gateway, but unmapped attributes are not shipped with preconfigured OIM metadata such as form fields, process tasks, or reconciliation mappings.

Custom attributes require additional configuration steps in the LDAP Gateway. See Section 5.1, "Adding Custom Fields for Target Resource Reconciliation" through Section 5.3, "Adding Custom Fields for Provisioning" for more information.

Table 1–3 lists the major differences between attribute types.

Table 1–3 Attribute Characteristics

Attribute Type	Out-of-the-box OIM Metadata Support	Out-of-the-box LDAP Support	Additional LDAP Configuration Required
Mapped	Yes	Yes	No
Unmapped	No	Yes	No
Custom	No	No	Yes

Table 1–4 lists mapped attribute mappings between CA Top Secret and Oracle Identity Manager. The OnBoardUser and ModifyTopsUser adapters are used for Create User and Modify User provisioning operations, respectively.

Table 1–4 Mapped User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	CA Top Secret Attribute Display Name	Description
USER_ID	USER	Login ID of the user
FULL_NAME	NAME	Full name of the user You can specify the format in which Full Name values are stored on the target system. Step 3 of Section 2.6, "Installing and Configuring the LDAP Gateway"describes the procedure.
Password	PASSWORD	Password
department	DEPARTMENT	Default department of the user **Note:** Provisioning is done using "department" attribute but reconciliation brings department's full name in "department" attribute and the acid value is brought in DEPTACID.

Table 1–4 (Cont.) Mapped User Attributes for Target Resource Reconciliation and Provisioning

Process Form Field	CA Top Secret Attribute Display Name	Description
deptacid	DEPARTMENT	Default department of the user **Note:** Provisioning is done using "department" attribute but reconciliation brings department's full name in "department" attribute and the acid value is brought in DEPTACID.
instdata	DATA	Installation-defined data of the user
createdate	CREATED	Date user was created
passwordExpire	EXPIRES	Expire the user's password
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
divacid	DIVISION	Default division for the user **Note:** Provisioning is done using "division" attribute but reconciliation brings division's full name in "division" attribute and the acid value is brought in "divacid."
division	DIVISION	Default division for the user **Note:** Provisioning is done using "division" attribute but reconciliation brings division's full name in "division" attribute and the acid value is brought in "divacid."
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
tsolacct	ACCTNUM	Default TSO account number on the TSO/E logon panel
tsohclass	HOLDCLASS	Default hold class
tsojclass	JOBCLASS	Default job class
tsomsize	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
tsoopt	OPT	TSO options, such as MAIL and NOTICES
tsosclass	SYSOUTCLASS	Default SYSOUT class
zone	ZONE	Display name of default zone for the user
zoneAcid	ZONE ACID	Default zone for the user

The Top Secret connector supports provisioning and reconciliation of additional attributes that are not included on the main process form or preconfigured with process tasks and reconciliation mappings.

Table 1–5 lists unmapped attribute mappings between CA Top Secret and Oracle Identity Manager. The adpModifyTopsUser adapter is used for Modify User provisioning operations, respectively.

Table 1–5 Unmapped User Attributes for Target Resource Reconciliation and Provisioning

LDAP Gateway Name	CA Top Secret Attribute	Description	Supported Operations
lu62#appl	#APPL	LU 6.2 #APPL	Both
lu62#entity	#ENTITY	LU 6.2 #ENTITY	Both
lu62bc1chain	BC1CHAIN	LU 6.2 BC1CHAIN	Both
lu62bc2chain	BC2CHAIN	LU 6.2 BC2CHAIN	Both
lu62set1disp	SET1DISP	LU 6.2 SET1DISP	Both
lu62set2disp	SET2DISP	LU 6.2 SET2DISP	Both
waaccnt	WAACCNT	APPC SYSOUT ACCT NUMBER	Both
waaddr1	WAADDR1	APPC SYSOUT ADDRESS 1	Both
waaddr2	WAADDR2	APPC SYSOUT ADDRESS 2	Both
waaddr3	WAADDR3	APPC SYSOUT ADDRESS 3	Both
waaddr4	WAADDR4	APPC SYSOUT ADDRESS 4	Both
wabldg	WABLDG	APPC SYSOUT BUILDING	Both
wadept	WADEPT	APPC SYSOUT DEPARTMENT	Both
waname	WANAME	APPC SYSOUT NAME	Both
waroom	WAROOM	APPC SYSOUT ROOM	Both
tsodefprfg	TSODEFPRFG	DEFAULT PERFORMANCE GROUP	Both
tsompw	TSOMPW	MULTIPLE PASSWORDS	Both **NOTE:** In reconciliation, the attribute is stored as "attributes" with value of "TSOMPW".
tsoacct	TSOACCT	SECURE TSO LOGON ACCOUNT CODES	Provisioning Only
tsoauth	TSOAUTH	SECURE TSO USER ATTRIBUTES	Provisioning Only
tsoprfg	TSOPRFG	SECURE TSO PERFORMANCE GROUPS	Provisioning Only
tsoproc	TSOPROC	SECURE TSOP LOGON PROCS	Provisioning Only
defaultGroup	DFLTGRP	OMVS DEFAULT GROUP	Both
omvsProgram	OMVSPGM	OMVS PROGRAM	Both
omvsUid	UID	OMVS USER ID	Both
omvsHome	HOME	OMVS HOME SUBDIRECTORY	Both
omvsGid	GID	OMVS GROUP ID	Both

Table 1–5 (Cont.) Unmapped User Attributes for Target Resource Reconciliation and Provisioning

LDAP Gateway Name	CA Top Secret Attribute	Description	Supported Operations
omvsAssize	ASSIZE	OMVS MAX ADDRESS SPACE SIZE	Both
omvsMmaparea	MMAPAREA	OMVS MAX DATASPACE PAGES	Both
omvsOecputm	OECPUTM	OMVS MAX CPU TIME	Both
omvsoefilep	OEFILEP	OMVS MAX FILES PER PROCESS	Reconciliation Only
omvsProcuser	PROCUSER	OMVS MAX PROCESSES	Both
omvsThreads	THREADS	OMVS MAX PTHREADS CREATED	Both
netviewMsgrecvr	MSGRECVR	NETVIEW RECEIVE UNSOLICITED MESSAGES	Both
netviewInitcmd	IC	NETVIEW INITIAL COMMAND	Both
netviewControl	CTL	NETVIEW SECURITY CHECK TYPE	Both
netviewOpclass	OPCLASS	NETVIEW SCOPE CLASS	Both
netviewDomains	DOMAINS	NETVIEW CROSS-DOMAIN SESSIONS	Both
netviewNgmfadmn	NGMFADMN	NETVIEW GRAPHICAL DISPLAY ADMIN	Both
netviewConsName	CONSNAME	NETVIEW EXTENDED CONSOLE NAME	Both
cicsOpclass	OPCLASS	CICS OPERATOR CLASSES	Both
cicsOpident	OPIDENT	CICS OPERATOR IDENTIFICATION VALUE	Both
cicsOpprty	OPPRTY	CICS OPERATOR PRIORITY	Both
cicsSctykey	SCTYKEY	CICS SECURITY KEYS	Both
cicsSitran	SITRAN	CICS TRANSACTION FOLLOWING FACILITY SIGN-IN	Both **Note:** To provision cicsSitran, you must map the process task to the adpModifySitranTopsUser adapter instead of adpModifyTopsUs.
cicsSitranFacility	SITRAN FACILITY	CICS FACILITY ASSOCIATED WITH TRANSACTION	Both **Note:** To provision cicsSitranFacility, you must map the process task to the adpModifySitranTopsUser adapter instead of adpModifyTopsUser.
misc1	MISC1	ADMIN MISC	Reconciliation Only
misc2	MISC2	ADMIN MISC	Reconciliation Only
misc3	MISC3	ADMIN MISC	Reconciliation Only
misc4	MISC4	ADMIN MISC	Reconciliation Only

Table 1–5 (Cont.) Unmapped User Attributes for Target Resource Reconciliation and Provisioning

LDAP Gateway Name	CA Top Secret Attribute	Description	Supported Operations
misc5	MISC5	ADMIN MISC	Reconciliation Only
misc7	MISC7	ADMIN MISC	Reconciliation Only
misc8	MISC8	ADMIN MISC	Reconciliation Only
misc9	MISC9	ADMIN MISC	Reconciliation Only

1.5.4 PROFILE Attributes for Target Resource Reconciliation and Provisioning

The connector supports reconciliation and provisioning of the PROFILE multivalued attribute. For any particular user, a child form is used to hold values of the PROFILE attributes listed in the table.

The AddUserToProfile and RemoveUserFromProfile adapters are used for PROFILE provisioning operations. Table 1–6 lists PROFILE attribute mappings between CA Top Secret and Oracle Identity Manager.

Table 1–6 PROFILE Attribute Mappings

Child Form Field	CA Top Secret Attribute	Description
UD_TSSPROF_ID	PROFILE	Profile ID

1.5.5 GROUP Attributes for Target Resource Reconciliation and Provisioning

The connector supports reconciliation and provisioning of the GROUP multivalued attribute. For any particular user, a child form is used to hold values of the GROUP attributes listed in the table.

The AddUserToGroup and RemoveUserFromGroup adapters are used for GROUP provisioning operations.

Table 1–7 lists GROUP attribute mappings between CA Top Secret and Oracle Identity Manager.

Table 1–7 GROUP Attribute Mappings

Child Form Field	CA Top Secret Attribute	Description
UD_TSSGROUP_ID	GROUP	Group ID

1.5.6 SOURCE Attributes for Provisioning

The connector supports provisioning of the SOURCE multivalued attribute. For any particular user, a child form is used to hold values of the SOURCE attributes listed in the table.

The AddUserToSource and RemoveUserFromSource adapters are used for SOURCE provisioning operations. Table 1–8 lists SOURCE attribute mappings between CA Top Secret and Oracle Identity Manager.

Table 1–8 SOURCE Attribute Mappings

Child Form Field	CA Top Secret Attribute	Description
UD_TSSSOURC_ID	SOURCE	Source ID

1.5.7 FACILITY Attributes for Target Resource Reconciliation and Provisioning

The connector supports reconciliation and provisioning of the FACILITY multivalued attribute. For any particular user, a child form is used to hold values of the FACILITY attributes listed in the table.

The AddUserToFacility and RemoveUserFromFacility adapters are used for FACILITY provisioning operations. Table 1–9 lists FACILITY attribute mappings between CA Top Secret and Oracle Identity Manager.

Table 1–9 FACILITY Attribute Mappings

Child Form Field	CA Top Secret Attribute	Description
UD_TSSFAC_ID	FACILITY	Facility ID

1.5.8 DATASET Attributes for Provisioning

The connector supports provisioning of the DATASET multivalued attribute. For any particular user, a child form is used to hold values of the DATASET attributes listed in the table.

The AddUserToDataset and RemoveUserFromDataset adapters are used for DATASET provisioning operations. Table 1–10 lists DATASET attribute mappings between CA Top Secret and Oracle Identity Manager.

Table 1–10 DATASET Attribute Mappings

Child Form Field	CA Top Secret Attribute	Description
DATASET_ID	DATASET	Dataset ID
DATASET_ACCESS	ACCESS	Users level of access to the dataset

1.5.9 Provisioning GENCERT Operations

The connector supports provisioning operations for the TSS GENCERT command, however a pre-configured child form, process task, and adapter are not included in with the release. To provision GENCERT actions, the OIM administrator will need to create an adapter and map it to the GenerateCertificate function in the topsecret-provisioning-adapter.jar file. Below is the function header for GenerateCertificate:

```
public String generateCertificate(String idfUserId, String digicert, String dcdsn,
String keysize, String keyusage,String nbdate, String nbtime, String nadate,
String natime, String lablcert, String altname, String subjects, String signwith,
String icsf, String dsa, String pcicc)
```

For boolean attributes such as ICSF or DSA, the administrator should map these values as literal String values equal to either true or false.

1.5.10 Provisioning GENREQ Operations

The connector supports provisioning operations for the TSS GENREQ command, however a pre-configured child form, process task, and adapter are not included in with the release. To provision GENREQ actions, the OIM administrator will need to create an adapter and map it to the GenerateCertificateRequest function in the topsecret-provisioning-adapter.jar file. Below is the function header for GenerateCertificateRequest:

```
public String generateCertificateRequest(String idfUserId, String digicert, String
dcdsn, String lablcert)
```

1.5.11 Reconciliation Rule

> **See Also:** *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for generic information about reconciliation matching and action rules

During target resource reconciliation, Oracle Identity Manager tries to match each user fetched from CA Top Secret with existing CA Top Secret resources provisioned to OIM Users. This is known as process matching. A reconciliation rule is applied for process matching. If a process match is found, then changes made to the user on the target system are copied to the resource on Oracle Identity Manager. If no match is found, then Oracle Identity Manager tries to match the user against existing OIM Users. This is known as entity matching. The reconciliation rule is applied during this process. If an entity match is found, then a CA Top Secret resource is provisioned to the OIM User. Data for the newly provisioned resource is copied from the user.

Rule name: IdfReconUserRule

Rule element: User Login Equals uid

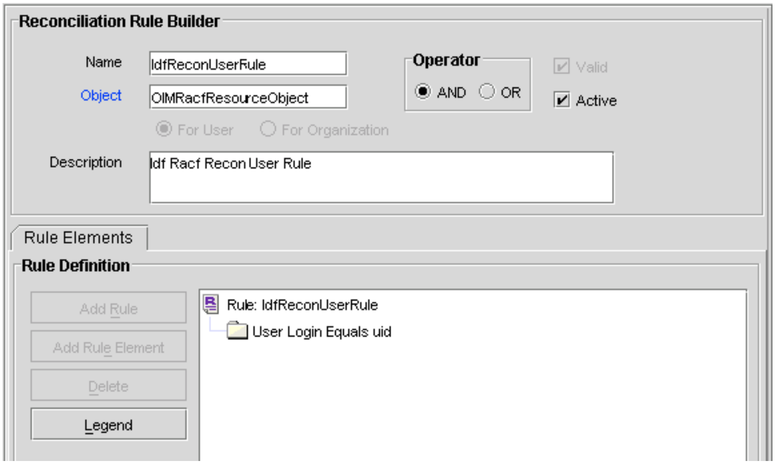
In this rule element:

- User Login is the User ID field on the process form and the OIM User form.
- uid is the USER attribute on CA Top Secret.

After you deploy the connector, you can view this reconciliation rule by performing the following steps:

1. On the Design Console, expand **Development Tools** and then double-click **Reconciliation Rules**.
2. Search for and open the **IdfReconUserRule** rule. Figure 1–4 shows this rule.

Figure 1–4 Reconciliation Rule



Reconciliation Rule Builder

Name: IdfReconUserRule

Object: OIMRacfResourceObject

● For User ○ For Organization

Operator: ● AND ○ OR

☑ Valid

☑ Active

Description: Idf Racf Recon User Rule

Rule Elements

Rule Definition

Rule: IdfReconUserRule

User Login Equals uid

1.5.12 Reconciliation Action Rules

Reconciliation action rules specify actions that must be taken depending on whether or not matching CA Top Secret resources or OIM Users are found when the reconciliation

)

rule is applied. Table 1–11 lists the reconciliation action rules.

Table 1–11 Reconciliation Action Rules

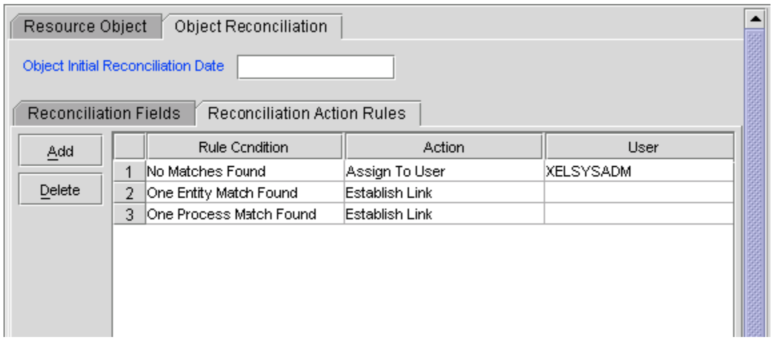
Rule Condition	Action
No Matches Found	None
One Entity Match Found	Establish Link
One Process Match Found	Establish Link

> **Note:** No action is performed for rule conditions that are not predefined for this connector. You can define your own action rule for such rule conditions. For information about modifying or creating reconciliation action rules, see *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager*.

After you deploy the connector, you can view the reconciliation action rules for target resource reconciliation by performing the following steps:

1. On the Design Console, expand **Resource Management** and then double-click **Resource Objects**.
2. Search for and open the **OIMTopSecretResourceObject** resource object.
3. Click the **Object Reconciliation** tab, and then click the **Reconciliation Action Rules** tab. The Reconciliation Action Rules tab displays the action rules defined for this connector. Figure 1–5 shows the reconciliation action rule for target resource reconciliation.

Figure 1–5 Reconciliation Action Rules



	Rule Ccndition	Action	User
1	No Matches Found	Assign To User	XELSYSADM
2	One Entity Match Found	Establish Link	
3	One Process Match Found	Establish Link	

2

Connector Deployment on Oracle Identity Manager

The LDAP Gateway acts as the intermediary between Oracle Identity Manager and the connector components on the mainframe. The following sections of this chapter describe the procedure to deploy some components of the connector, including the LDAP Gateway, on the Oracle Identity Manager host computer:

> **Note:** The procedure to deploy the mainframe components of the connector is described in the next chapter.

- Section 2.1, "Files and Directories That Comprise the Connector"
- Section 2.2, "Running the Connector Installer"
- Section 2.3, "Configuring the IT Resource"
- Section 2.4, "Configuring Oracle Identity Manager"
- Section 2.5, "Configuring Oracle Identity Manager for Request-Based Provisioning"
- Section 2.6, "Installing and Configuring the LDAP Gateway"

2.1 Files and Directories That Comprise the Connector

Table 2–1 describes the files and directories on the installation media.

Table 2–1 Files and Directories That Comprise the Connector

Files and Directories	Description
configuration/TopsAdv.xml	This XML file contains configuration information that is used during connector installation.
DataSets/ProvisionResource_OIMTopsResourceObject.xml DataSets/ModifyProvisionedResource_OIMTopsResourceObject	This XML file specifies the information to be submitted by the requester during a request-based provisioning operation. Section 2.5, "Configuring Oracle Identity Manager for Request-Based Provisioning" provides more information. **Note:** The dataset XML files are applicable only if you are using Oracle Identity Manager release 11.1.1.*x*
etc/LDAP Gateway/ldapgateway.zip	This ZIP file contains the files required to deploy the LDAP Gateway.

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

Files and Directories	Description
etc/Provisioning and Reconciliation Connector/Mainframe_TS.zip	This ZIP file contains the files required to deploy the Reconciliation and Provisioning Agents on the mainframe. Section 3.2, "Deploying the Reconciliation Agent and Provisioning Agent" describes the files bundled in this ZIP file.
lib/topsecret-provisioning-adapter.jar	This JAR file contains the code for the adapters that are used during connector provisioning operations. During connector installation, this file is copied to the Oracle Identity Manager database.
Files in the resources directory	Each of these resource bundles contains locale-specific information that is used by the connector. During connector installation, this file is copied to the Oracle Identity Manager database. Note: A resource bundle is a file containing localized versions of the text strings that include GUI element labels and messages.
scripts/propertyEncrypt.bat scripts/propertyEncrypt.sh	You use this script to encrypt passwords that you enter in the beans.xml files. Section 2.6, "Installing and Configuring the LDAP Gateway" provides more information.
lib/topsecret-scheduled-tasks.jar	This JAR file contains the code for the connector's scheduled tasks that perform lookup population and full reconciliation. During connector installation, this file is copied to the Oracle Identity Manager database.
xml/oimTopsAdvConnector.xml	This XML file contains definitions of the connector components, such as the IT resource and resource object. These objects are created in Oracle Identity Manager when you import the XML file.
upgrade/PostUpgradeScriptTops.sql	This file is used during the connector upgrade procedure for Oracle Identity Manager release 11.1.2.*x.*

2.2 Running the Connector Installer

To run the Connector Installer:

1. Copy the contents of the connector installation media directory into the following directory:

   OIM_HOME/server/ConnectorDefaultDirectory

2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 11.1.1.*x:*

     a. Log in to Oracle Identity System Administration by using the user account described in the Creating the User Account for Installing Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

     b. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Manage Connector**.

   - For Oracle Identity Manager release 11.1.2.*x:*

     a. Log in to Oracle Identity System Administration by using the user account described in the Creating the User Account for Installing Connectors in *Oracle Fusion Middleware Administering Oracle Identity Manager.*

   b. In the left pane, under System Management, click **Manage Connector.**

3. In the Manage Connector page, click **Install.**
4. From the Connector list, select **CA Top Secret Advanced** ***RELEASE_NUMBER.*** This list displays the names and release numbers of connectors whose installation files you copy into the default connector installation directory in Step 1.

   If you have copied the installation files into a different directory, then:

   a. In the **Alternative Directory** field, enter the full path and name of that directory.

   b. To repopulate the list of connectors in the Connector list, click **Refresh.**

   c. From the Connector list, select **CA Top Secret Advanced** ***RELEASE_NUMBER.***
5. Click **Load.**
6. To start the installation process, click **Continue.**

   The following tasks are performed in sequence:

   a. Configuration of connector libraries.

   b. Import of the connector Target Resource user configuration XML file (by using the Deployment Manager).

   c. Compilation of adapters.

   On successful completion of a task, a check mark is displayed for the task. If a task fails, then an X mark and a message stating the reason for failure are displayed. Depending on the reason for the failure, make the required correction and then perform one of the following steps:

   - Retry the installation by clicking **Retry.**
   - Cancel the installation and begin again from Step 1.
7. If all three tasks of the connector installation process are successful, then a message indicating successful installation is displayed. In addition, a list of the steps that you must perform after the installation is displayed. These steps are as follows:

   a. Ensuring that the prerequisites for using the connector are addressed.

   > **Note:** At this stage, run the Oracle Identity Manager PurgeCache utility to load the server cache with content from the connector resource bundle in order to view the list of prerequisites. See Section 2.4.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for information about running the PurgeCache utility.
   >
   > There are no prerequisites for some predefined connectors.

   b. Configuring the IT resource for the connector.

   Record the name of the IT resource displayed on this page. The procedure to configure the IT resource is described later in this guide.

   c. Configuring the scheduled jobs that are created when you installed the connector.

Record the names of the scheduled jobs displayed on this page. The procedure to configure these scheduled jobs is described later in this guide.

When you run the Connector Installer, it copies the connector files and external code files to destination directories on the Oracle Identity Manager host computer. These files are listed in Table 2–1.

Installing the Connector in an Oracle Identity Manager Cluster

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the `resources` directory into the corresponding directories on each node of the cluster. See Section 2.1, "Files and Directories That Comprise the Connector" for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

2.3 Configuring the IT Resource

You must specify values for the parameters of the TopSecretResource IT resource as follows:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
    - For Oracle Identity Manager release 11.1.1.*x:*
        a. Log in to the Oracle Identity System Administration.
        b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
        c. On the Welcome to Oracle Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource.**
    - For Oracle Identity Manager release 11.1.2.*x:*
        a. Log in to the Oracle Identity System Administration.
        b. In the left pane, under Configuration, click **IT Resource.**
2. In the IT Resource Name field on the Manage IT Resource page, enter `TopSecretResource` and then click **Search.**
3. Click the edit icon for the IT resource.
4. From the list at the top of the page, select **Details and Parameters.**
5. Specify values for the parameters of the IT resource. Table 2–2 describes each parameter.

Table 2–2 IT Resource Parameters

Parameter	Description
AtMap User	This parameter holds the name of the lookup definition containing attribute mappings that are used for provisioning. Value: `AtMap.TOPS` **Note:** You must not change the value of this parameter.
idfPrincipalDn	Set a user ID for an account that the connector will use to connect to the LDAP Gateway. Format: `cn=`*`USER_ID`*`,dc=tops,dc=com` Sample value: `cn=idfTopsAdmin,dc=tops,dc=com` You also set this user ID in the beans.xml inside the idfserver.jar file. See Step 5 in Section 2.6, "Installing and Configuring the LDAP Gateway."
idfPrincipalPwd	Set a password for the account that the connector will use to connect to the LDAP Gateway. You also set this password in the files listed in the description of the idfPrincipalDn parameter. **Note:** Do not enter an encrypted value.
idfRootContext	This parameter holds the root context for CA Top Secret. Value: `dc=tops,dc=com` **Note:** You must not change the value of this parameter.
idfServerHost	This parameter holds the host name or IP address of the computer on which you install the LDAP Gateway. For this release of the connector, you install the LDAP Gateway on the Oracle Identity Manager host computer. Default value: `localhost` **Note:** Do not change the value of this parameter unless you have installed the LDAP Gateway on a different machine from the Oracle Identity Manager host computer.
idfServerPort	Enter the number of the port for connecting to the LDAP Gateway. Sample value: `5389` You also set this port number in the beans.xml inside the idfserver.jar file. See Step 5 in Section 2.6, "Installing and Configuring the LDAP Gateway."
idfSsl	This parameter determines whether the LDAP Gateway will use SSL to connect to the target system. Enter `true` if using SSL. Otherwise, enter `false`. Sample value: `true`
idfTrustStore	This parameter holds the directory location of the trust store containing the SSL certificate. This parameter is optional, and should only be entered when using SSL authentication. This must be the full path to the directory location. Sample value: `/app/home/ldapgateway/conf/idf.jks`

Table 2–2 (Cont.) IT Resource Parameters

Parameter	Description
idfTrustStorePassword	This parameter holds the password for the SSL trust store. This parameter is optional, and should only be entered when using SSL authentication.
idfTrustStoreType	This parameter holds the trust store type for the SSL trust store. This parameter is optional, and should only be entered when using SSL authentication. Sample value: `jks`
Last Modified Time Stamp	The most recent start time of the Reconcile LDAP Users reconciliation scheduled task is stored in this parameter. See Section 4.4.2.4, "Top Secret Reconcile All LDAP Users" for more information about his scheduled task. The format of the value stored in this parameter is as follows: MM/dd/yy hh:mm:ss a In this format: MM is the month of the year. dd is the day of the month. yy is the year. hh is the hour in am/pm (01-12). mm is the minute in the hour. ss is the second in the minute. a is the marker for AM or PM. Sample value: `05/07/10 02:46:52 PM` The default value is 0. The reconciliation task will perform full LDAP user reconciliation when the value is 0. If the value is a non-zero, standard time-stamp value in the format given above, then incremental reconciliation is performed. Only records that have been created or modified after the specified time stamp are brought to Oracle Identity Manager for reconciliation. **Note:** When required, you can manually enter a time-stamp value in the specified format.

6. To save the values, click **Update.**

2.4 Configuring Oracle Identity Manager

Configuring Oracle Identity Manager involves the following procedures:

> **Note:** In an Oracle Identity Manager cluster, you must perform these steps on each node of the cluster.

- Section 2.4.1, "Configuring Oracle Identity Manager 11.1.2 or Later"
- Section 2.4.2, "Localizing Field Labels in UI Forms"
- Section 2.4.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache"
- Section 2.4.4, "Enabling Logging"

2.4.1 Configuring Oracle Identity Manager 11.1.2 or Later

If you are using Oracle Identity Manager release 11.1.2 or later, you must create additional metadata such as a UI form and an application instance. In addition, you must run entitlement and catalog synchronization jobs. These procedures are described in the following sections:

- Section 2.4.1.1, "Creating and Activating a Sandbox"
- Section 2.4.1.2, "Creating a New UI Form"
- Section 2.4.1.3, "Creating an Application Instance"
- Section 2.4.1.4, "Publishing a Sandbox"
- Section 2.4.1.5, "Harvesting Entitlements and Sync Catalog"
- Section 2.4.1.6, "Updating an Existing Application Instance with a New Form"

2.4.1.1 Creating and Activating a Sandbox

Create and activate a sandbox as follows. For detailed instructions, see the Managing Sandboxes in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. On the upper navigation bar, click **Sandboxes.** The Manage Sandboxes page is displayed.
2. On the toolbar, click **Create Sandbox.** The Create Sandbox dialog box is displayed.
3. In the Sandbox Name field, enter a name for the sandbox. This is a mandatory field.
4. In the Sandbox Description field, enter a description of the sandbox. This is an optional field.
5. Click **Save and Close.** A message is displayed with the sandbox name and creation label.
6. Click **OK.** The sandbox is displayed in the Available Sandboxes section of the Manage Sandboxes page.
7. From the table showing the available sandboxes in the Manage Sandboxes page, select the newly created sandbox that you want to activate.
8. On the toolbar, click **Activate Sandbox.**

   The sandbox is activated.

2.4.1.2 Creating a New UI Form

Create a new UI form as follows. For detailed instructions, see the Managing Forms chapter in the Managing Forms in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. In the left pane, under Configuration, click **Form Designer.**
2. Under Search Results, click **Create.**
3. Select the resource type for which you want to create the form, for example, **OIMTopSecretResourceObject.**
4. Enter a form name and click **Create.**

2.4.1.3 Creating an Application Instance

Create an application instance as follows. For detailed instructions, see the Managing Application Instances in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

1. In the System Administration page, under Configuration in the left pane, click **Application Instances.**
2. Under Search Results, click **Create.**
3. Enter appropriate values for the fields displayed on the Attributes form and click **Save.**
4. In the Form drop-down list, select the newly created form and click **Apply.**
5. Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See Modifying Application Instances section in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed instructions.

2.4.1.4 Publishing a Sandbox

To publish the sandbox that you created in Section 2.4.1.1, "Creating and Activating a Sandbox":

1. Close all the open tabs and pages.
2. In the upper-right corner of the page, click the Sandboxes link.

   The Manage Sandboxes page is displayed.
3. From the table showing the available sandboxes in the Manage Sandboxes page, select the sandbox that you created in Section 2.4.1.1, "Creating and Activating a Sandbox."
4. On the toolbar, click **Publish Sandbox.** A message is displayed asking for confirmation.
5. Click **Yes** to confirm. The sandbox is published and the customizations it contained are merged with the main line.

2.4.1.5 Harvesting Entitlements and Sync Catalog

To harvest entitlements and sync catalog:

1. Run the scheduled jobs for lookup field synchronization. See Section 4.2, "Scheduled Tasks for Lookup Field Synchronization" for more information about these scheduled jobs.
2. Run the Entitlement List scheduled job to populate Entitlement Assignment schema from child process form table. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.
3. Run the Catalog Synchronization Job scheduled job. See Predefined Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about this scheduled job.

2.4.1.6 Updating an Existing Application Instance with a New Form

For any changes you do in the Form Designer, you must create a new UI form and update the changes in an application instance. To update an existing application instance with a new form:

1. Create a sandbox and activate it as described in Section 2.4.1.1, "Creating and Activating a Sandbox."
2. Create a new UI form for the resource as described in Section 2.4.1.2, "Creating a New UI Form."
3. Open the existing application instance.
4. In the **Form** field, select the new UI form that you created.
5. Save the application instance.
6. Publish the sandbox as described in Section 2.4.1.4, "Publishing a Sandbox."

2.4.2 Localizing Field Labels in UI Forms

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.2.*x*, and you want to localize UI form field labels.

To localize field label that is added to the UI forms:

1. Log in to Oracle Enterprise Manager.
2. In the left pane, expand **Application Deployments** and then select **oracle.iam.console.identity.sysadmin.ear.**
3. In the right pane, from the Application Deployment list, select **MDS Configuration.**
4. On the MDS Configuration page, click **Export** and save the archive to the local computer.
5. Extract the contents of the archive, and open the following file in a text editor: For Oracle Identity Manager 11g Release 2 PS2 (11.1.2.2.0) and later:

   SAVED_LOCATION\xliffBundles\oracle\iam\ui\runtime\BizEditorBundle.xlf
6. Edit the BizEditorBundle.xlf file as follows:

   a. Search for the following text:

   ```
   <file source-language="en"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   b. Replace with the following text:

   ```
   <file source-language="en" target-language="LANG_CODE"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   In this text, replace *LANG_CODE* with the code of the language that you want to localize the form field labels. The following is a sample value for localizing the form field labels in Japanese:

   ```
   <file source-language="en" target-language="ja"
   original="/xliffBundles/oracle/iam/ui/runtime/BizEditorBundle.xlf"
   datatype="x-oracle-adf">
   ```

   c. Search for the application instance code. The original code will be in the following format:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_<Field_Name>__c_description']}">
<source><Field_Label></source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.<UI_Form_Name>.entity.
<UI_Form_Name>EO.UD_<Field_Name>__c_LABEL">
<source><Field_Label></source>
<target/>
</trans-unit>
```

For example, the following sample code show the update that should be made for the FULL NAME field on a UI form named TopSecretUserFormv1:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_IDF_TOPS_CN__c_description']}">
<source>FULL NAME</source>
<target/>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.TopSecretUserFormv1.entity.
TopSecretUserFormv1EO.UD_IDF_TOPS_CN__c_LABEL">
<source>FULL NAME
</source>
<target/>
</trans-unit>
```

d. Open the resource file from the /resources directory in the connector installation media, for example TopSecret-Adv_ja.properties, and get the value of the attribute from the file, for example global.udf.UD_IDF_TOPS_CN=\u6C0F\u540D.

e. Replace the original code shown in Step 6.c with the following:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_<Field_Name>__c_description']}">
<source>< global.udf.UD_Field_Name></source>
<target/>enter Unicode values here</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.<UI_Form_Name>.entity.
<UI_Form_Name>EO.UD_<Field_Name>__c_LABEL">
<source><Field_Label></source>
<target/>enter Unicode values here</target>
</trans-unit>
```

As an example, the code for FULL_NAME field translation would be:

```
<trans-unit
id="${adfBundle['oracle.adf.businesseditor.model.util.BaseRuntimeResourceBu
ndle']['persdef.sessiondef.oracle.iam.ui.runtime.form.model.user.entity.use
rEO.UD_IDF_TOPS_CN__c_description']}">

<source>FULL_NAME</source>
```

```
<target>\u6C0F\u540D</target>
</trans-unit>
<trans-unit
id="sessiondef.oracle.iam.ui.runtime.form.model.TopSecretUserFormv1.entity.
TopSecretUserFormv1EO.UD_IDF_TOPS_CN__c_LABEL">
<source>FULL_NAME</source>
<target>\u6C0F\u540D</target>
</trans-unit>
```

f. Repeat Steps 6.c through 6.e for all attributes of the process form.

g. Save the file as BizEditorBundle_LANG_CODE.xlf. In this file name, replace *LANG_CODE* with the code of the language to which you are localizing. Sample file name: `BizEditorBundle_ja.xlf`.

7. Repackage the ZIP file and import it into MDS.

8. Log out of and log in to Oracle Identity Manager.

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

When you deploy the connector, the resource bundles are copied from the resources directory on the installation media into Oracle Identity Manager database. Whenever you add a new resource bundle to 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, switch to the *OIM_HOME*/server/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/server/bin/SCRIPT_FILE_NAME
```

2. Enter one of the following commands:

Note: You can use the PurgeCache utility to purge the cache for any content category. Run `PurgeCache.bat` *CATEGORY_NAME* on Microsoft Windows or `PurgeCache.sh` *CATEGORY_NAME* on UNIX. The *CATEGORY_NAME* argument represents the name of the content category that must be purged.

For example, the following commands purge Metadata entries from the server cache:

```
PurgeCache.bat MetaData
```

```
PurgeCache.sh MetaData
```

- On Microsoft Windows: `PurgeCache.bat All`
- On UNIX: `PurgeCache.sh All`

When prompted, enter the user name and password of an account belonging to the SYSTEM ADMINISTRATORS group. In addition, you are prompted to enter the service URL in the following format:

```
t3://OIM_HOST_NAME:OIM_PORT_NUMBER
```

In this format:

- Replace *OIM_HOST_NAME* with the host name or IP address of the Oracle Identity Manager host computer.
- Replace *OIM_PORT_NUMBER* with the port on which Oracle Identity Manager is listening.

See *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the PurgeCache utility.

2.4.4 Enabling Logging

The CA Top Secret connector supports two forms of logging, namely LDAP gateway-level logging and Oracle Identity Manager-level logging. This section discusses the following topics:

- Section 2.4.4.1, "Enabling Logging for the LDAP Gateway"
- Section 2.4.4.2, "Enabling Logging in Oracle Identity Manager"

2.4.4.1 Enabling Logging for the LDAP Gateway

LDAP Gateway logging operations are managed by the log4j.properties file, which can be extracted from within the ldapgateway/dist/idfserver.jar compilation (see step 10 of Section 2.6, "Installing and Configuring the LDAP Gateway"). In the log4j.properties file, edit the rootLogger log level:

```
log4j.rootLogger=ERROR
```

The following is a list of log levels that can be used:

- 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.

Multiple log files are available for use with the connector. Table 2–3 lists the name, location, and contents of each LDAP gateway log file.

Table 2–3 Log Files and their Contents

Log File	Description
nohup.out	This log file contains the console window output from the LDAP Gateway. This file is primarily used in conjunction with the run.sh script (instead of the run.bat file) **Location:** .../`ldapgateway/bin/`
idfserver.log.0	This log file contains provisioning and reconciliation logging messages from the LDAP Gateway and is the primary log file used by the gateway component. **Location:** .../`ldapgateway/logs/`

2.4.4.2 Enabling Logging in Oracle Identity Manager

Oracle Identity Manager uses Oracle Java Diagnostic Logging (OJDL) for logging. OJDL is based on java.util.logger. 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:

- SEVERE.intValue()+100

  This level enables logging of information about fatal errors.

- SEVERE

  This level enables logging of information about errors that might allow Oracle Identity Manager to continue running.

- WARNING

  This level enables logging of information about potentially harmful situations.

- INFO

  This level enables logging of messages that highlight the progress of the application.

- CONFIG

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

- FINE, FINER, FINEST

  These levels enable logging of information about fine-grained events, where FINEST logs information about all events.

These log levels are mapped to ODL message type and level combinations as shown in Table 2–4.

Table 2–4 Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
SEVERE.intValue()+100	INCIDENT_ERROR:1
SEVERE	ERROR:1
WARNING	WARNING:1

Table 2–4 (Cont.) Log Levels and ODL Message Type:Level Combinations

Log Level	ODL Message Type:Level
INFO	NOTIFICATION:1
CONFIG	NOTIFICATION:16
FINE	TRACE:1
FINER	TRACE:16
FINEST	TRACE:32

OIM level logging operations are managed by the logging.xml file, which is located in following directory:

DOMAIN_NAME/config/fmwconfig/servers/*SERVER_NAME*/

Loggers are used to configure logging operations for the connector's OIM functions. To configure loggers:

1. In the text editor, open the *DOMAIN_NAME*/config/fmwconfig/servers/*SERVER_NAME*/logging.xml file.
2. Locate the logger you want to configure. If adding a logger for the first time, you must create the logger definition. Table 2–5, " Logger Parameters" lists the Oracle Identity Manager loggers for this connector.

Table 2–5 Logger Parameters

Logger	Description
COM.IDENTITYFORGE.IDFTOPSUSEROPERATIONS	Logs events related to provisioning operations from Oracle Identity Manager to the LDAP gateway, such as user creation and modification events.
COM.IDENTITYFORGE.UTIL.TOPS.IDFLDAPOPERATIONS	Logs events related to basic LDAP functions, including connecting to and disconnecting from the LDAP gateway.
COM.IDENTITYFORGE.TOPS.TASKS.FINDALLDATASETSTASK	Logs events related to the Find All Datasets scheduled task.
COM.IDENTITYFORGE.TOPS.TASKS.FINDALLFACILITIESTASK	Logs events related to the Find All Facilities scheduled task.
COM.IDENTITYFORGE.TOPS.TASKS.FINDALLGROUPSTASK	Logs events related to the Find All Groups scheduled task.
COM.IDENTITYFORGE.TOPS.TASKS.FINDALLPROFILESTASK	Logs events related to the Find All Profiles scheduled task.
COM.IDENTITYFORGE.TOPS.TASKS.FINDALLSOURCESTASK	Logs events related to the Find All Sources scheduled task.
COM.IDENTITYFORGE.TOPS.TASKS.RECONCILEALLLDAPUSERSTASK	Logs events related to the Reconcile All LDAP Users scheduled task.
COM.IDENTITYFORGE.TOPS.TASKS.RECONCILEUSERSTOINTERNALLDAPTASK	Logs events related to the CFILE extract from TSS to initialize users to the internal LDAP, reconcile users to internal LDAP scheduled task.
COM.IDENTITYFORGE.TOPS.TASKS.RECONCILEALLUSERSTASK	Logs events related to the Reconcile All Users scheduled task
COM.IDENTITYFORGE.TOPS.TASKS.RECONCILEDELETEDUSERSTOOIMTASK	Logs events related to the Reconcile Deleted Users to OIM scheduled task.

3. Define the <logger> element and its handlers. You can use the standard odl-handler as the log handler, or write your own. For more information on configuring logging in Oracle Identity Manager 11*g*, see Enabling Logging in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

   The following is an example of a logger definition for the Reconcile All Users scheduled task:

   ```
   <logger name="COM.IDENTITYFORGE.TOPS.TASKS.RECONCILEALLUSERSTASK"
   level='TRACE:32'>
   <handler name='odl-handler'/>
   </logger>
   ```

4. Save the changes and close the file.
5. Restart the Oracle Identity Manager server for the changes to take effect.

Log statements will be written to the path that is defined in the log handler that you assigned in the logger definition. For example, in the above logger definition for the Reconcile All Users scheduled task (in step3), the handler is odl-handler, which has the following default output file path:

```
${domain.home}/servers/${weblogic.Name}/logs/${weblogic.Name}-diagnostic.l
og'
```

2.5 Configuring Oracle Identity Manager for Request-Based Provisioning

> **Note:** Perform the procedure described in this section only if you are using Oracle Identity Manager release 11.1.1.*x* and you want to configure request-based provisioning.

In request-based provisioning, an end user creates a request for a resource by using the Oracle Identity System Administration. Administrators or other users can also create requests for a particular user. Requests for a particular resource on the resource can be viewed and approved by approvers designated in Oracle Identity Manager.

The following are features of request-based provisioning:

- A user can be provisioned only one resource (account) on the target system.

> **Note:** Direct provisioning allows the provisioning of multiple target system accounts on the target system.

- Direct provisioning cannot be used if you enable request-based provisioning.

To configure request-based provisioning, perform the following procedures:

- Section 2.5.1, "Copying Predefined Request Datasets"
- Section 2.5.2, "Importing Request Datasets into the MDS"
- Section 2.5.3, "Enabling the Auto Save Form Feature"
- Section 2.5.4, "Running the PurgeCache Utility"

2.5.1 Copying Predefined Request Datasets

A request dataset is an XML file that specifies the information to be submitted by the requester during a provisioning operation. Predefined request datasets are shipped with this connector. These request datasets specify information about the default set of attributes for which the requester must submit information during a request-based provisioning operation. The following predefined request datasets are available in the DataSets directory on the installation media:

ProvisionResource_OIMTopsResourceObject.xml

ModifyProvisionedResource_OIMTopsResourceObject

Copy these files from the installation media to any directory on the Oracle Identity Manager host computer. It is recommended that you create a directory structure as follows:

/custom/connector/*RESOURCE_NAME*

For example:

E:\MyDatasets\custom\connector\TopSecretAdv

> **Note:** Until you complete the procedure to configure request-based provisioning, ensure that there are no other files or directories inside the parent directory in which you create the directory structure. In the preceding example, ensure that there are no other files or directories inside the *E:\MyDatasets directory.*

The directory structure to which you copy the dataset files is the MDS location into which these files are imported after you run the Oracle Identity Manager MDS Import utility. The procedure to import dataset files is described in the next section.

Depending on your requirement, you can modify the file names of the request datasets. In addition, you can modify the information in the request datasets. See for information on modifying request datasets. *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager.*

2.5.2 Importing Request Datasets into the MDS

All request datasets must be imported into the metadata store (MDS), which can be done by using the Oracle Identity Manager MDS Import utility.

To import a request dataset definition into MDS:

1. Ensure that you have set the environment for running the MDS Import utility. See *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for detailed information about setting up the environment for MDS utilities.

> **Note:** While setting up the properties in the weblogic.properties file, ensure that the value of the metadata_from_loc property is the parent directory of the /custom/connector/*RESOURCE_NAME* directory. For example, while performing the procedure in Section 2.5.1, "Copying Predefined Request Datasets," if you copy the files to the E:\MyDatasets\custom\connector\TopSecretAdv directory, then set the value of the metada_from_loc property to `E:\MyDatasets`.

2. In a command window, change to the *OIM_HOME*\server\bin directory.
3. Run one of the following commands:
   - On Microsoft Windows

     ```
     weblogicImportMetadata.bat
     ```

   - On UNIX

     ```
     weblogicImportMetadata.sh
     ```

4. When prompted, enter the following values:
   - `Please enter your username [weblogic]`

     Enter the username used to log in to the WebLogic server

     Sample value: `WL_User`

   - `Please enter your password [weblogic]`

     Enter the password used to log in to the WebLogic server.

   - `Please enter your server URL [t3://localhost:7001]`

     Enter the URL of the application server in the following format:

     `t3://`*`HOST_NAME_IP_ADDRESS`*`:`*`PORT`*

     In this format, replace:

     – *HOST_NAME_IP_ADDRESS* with the host name or IP address of the computer on which Oracle Identity Manager is installed.

     – *PORT* with the port on which Oracle Identity Manager is listening.

   The request dataset is imported into MDS at the following location:

   /custom/connector/*RESOURCE_NAME*

2.5.3 Enabling the Auto Save Form Feature

To enable the Auto Save Form feature:

1. Log in to the Design Console.
2. Expand **Process Management,** and then double-click **Process Definition.**
3. Search for and open the **OIMTopsProvisioningProcess** process definition.
4. Select the **Auto Save Form** check box.
5. Click the Save icon.

2.5.4 Running the PurgeCache Utility

Run the PurgeCache utility to clear content belonging to the Metadata category from the server cache. See Section 2.4.3, "Clearing Content Related to Connector Resource Bundles from the Server Cache" for instructions.

The procedure to configure request-based provisioning ends with this step.

2.6 Installing and Configuring the LDAP Gateway

The IT resource contains connection information for Oracle Identity Manager to connect to the LDAP Gateway. The tops.properties file is one of the components of the gateway. This file contains information used by the gateway to connect to the mainframe. Configuring the gateway involves setting values in the tops.properties file and the other files that constitute the 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 you want to install the LDAP Gateway. This ZIP file is in the etc/LDAP Gateway directory on the installation media.

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

2. In a text editor, open the *LDAP_INSTALL_DIR*/conf/tops.properties file. The following table describes these properties.

Table 2–6 Properties in the tops.properties File

Property	Description
agentPort	Enter the port number on the LDAP Gateway host computer that you are going to reserve for messages sent from the mainframe by the Reconciliation Agent, Voyager. The LDAP Gateway will receive real-time reconciliation messages using this port. This value should match the value of the PORT parameter in the Voyager agent control file. See Table 3–13 in section 3.8, "Configuring the Started Tasks" for more information on the Voyager control file parameters.

configDNames	This property holds the name of any custom target system attributes that should be included when the LDAP gateway parses a user profile from the target system (typically performed during reconciliation). If you are using a target system attribute that is not supported out-of-the-box, then add the name of that attribute to the value of the configDNames property. The name should match the format of the attribute name when executing a LIST command on the target system and you must include the Spaces and = for each attribute. This step is mentioned in the following sections:
	■ Section 5.1, "Adding Custom Fields for Target Resource Reconciliation"
	■ Section 5.3, "Adding Custom Fields for Provisioning"
	For example, if you defined two Top Secret fields named PST15, and VEND, then you would enter:
	`# CONFIG DISPLAY NAMES`
	`configDNames =VEND =|PST15 =|`
	To enter multiple custom attributes, separate each entry with a vertical bar.

Table 2–6 (Cont.) Properties in the tops.properties File

<table>
<tr><th>Property</th><th>Description</th></tr>
<tr><td>configAttrs</td><td>This property holds the name of any custom target system attributes that should be included when the LDAP gateway parses a user profile from the target system (typically performed during reconciliation). If you are using a target system attribute that is not supported out-of-the-box, then add the name of that attribute to the value of the configAttrs property. The name should match the format of the attribute name when executing a LIST command on the target system but without the data from above in the configDNames and this is that will match your LDAP and OIM attribute name when configuring. This step is mentioned in the following sections:
■ Section 5.1, "Adding Custom Fields for Target Resource Reconciliation"
■ Section 5.3, "Adding Custom Fields for Provisioning"
For example, if you define three Top Secret fields named $PST15, PST VRO 16, and VEND ID, then you would enter:
<code># CONFIG ATTRIBUTES</code>
<code>configAttrs=$PST15|VEND|</code>
To enter multiple custom attributes, separate each entry with a vertical bar.</td></tr>
<tr><td>configDatasets</td><td>If you create a custom dataset on the target system, then add the name of that dataset type to the value of the configDatasets property.
For example:
<code># CONFIG DATASETS</code>
<code>configDatasets=$RAFT</code>
To enter multiple custom dataset names, separate each entry with a vertical bar.</td></tr>
<tr><td>customDataset</td><td>This property is used to store custom dataset names when issuing a WHOHAS command to the Top Secret system. If more than one custom dataset exists, separate each entry with a vertical bar ('|') character.
Custom datasets that are added to this property will be included when the dataset lookup synchronization task ('Top Secret Find All Datasets') is run in Oracle Identity Manager.
For example:
<code># CUSTOM DATASETS FOR WHOHAS COMMAND</code>
<code>_customDataset_$XRAFT|$RAFT|</code></td></tr>
<tr><td>defaultDelete</td><td>Enter one of the following as the value of this property:
■ Set revoke as the value 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 if you want the user to be deleted from the target system as the outcome of a Delete User provisioning operation.
For example:
<code># DEFAULT ACTION WHEN DELETE FUNCTION USED</code>
<code>defaultDelete=delete</code></td></tr>
<tr><td>host</td><td>Set the host name or IP address of the mainframe as the value of this property.</td></tr>
</table>

Table 2–6 (Cont.) Properties in the tops.properties File

Property	Description
port	Enter the number of the port on the mainframe that you are going to reserve for the Provisioning Agent. The LDAP Gateway will send provisioning messages to this port. This value should match the PORT parameter specified in the Pioneer provisioning agent STC. See Section 3.8, "Configuring the Started Tasks" for more information on the Pioneer STC.
ver45	This property is used to determine whether the LDAP gateway must use the large (240K) socket buffer when passing messages to the target system. Values: `[true|false]` If you set the value of this property to `true,` the LDAP gateway will use a 240K socket buffer. If you set the value of this property to `false,` the LDAP gateway will use a 32K socket buffer. Default setting is `true.`
stcID	This property is not supported from 9.0.4.18 and later releases of this connector. This property allows the real-time agent to ignore events that have been submitted to the target system by the Pioneer STC (such as by request from Oracle Identity manager). Enter the name given to the Pioneer STARTED TASK.
domainOu	This property stores users in the specified subtree under the ou=People tree of the internal LDAP store. This entry needs to be unique and specific for each system if multiple systems are used within one LDAP Gateway. Default setting is `domainOu=tops`
internalEnt	This property allows the real-time agent to store user data in the LDAP Gateway internal store. Values: `[true|false]`
useExtractUser	This property specifies whether messages sent to the Provisioning Agent (PIONEER) will use EXTRACT format. Values: `[true|false]` **Note:** Message format from the Reconciliation Agent (VOYAGER) is configured in the agent control file.

Table 2–6 (Cont.) Properties in the tops.properties File

Property	Description

ignoreChar	Use this property to specify characters in PROFILE names that must be ignored when retrieving user data from the LDAP Gateway. For example:
	Suppose User1 is a member of the TESTGRP1 profile until 01-Jan-2020. When a LIST function is called for User1, the output for the PROFILES section is `*TESTGRP1`.
	If you set the value of the ignoreChar property to *, then the LDAP Gateway ignores the asterisk character in the name of the profile. In other words, when the LIST function is called, the output for the PROFILES section is `TESTGRP1`.
	You can set multiple characters to be ignored as the value of the ignoreChar property. Do not use any blank character or space as the delimiter for the set of characters that you specify. For example, if you want both the asterisk character and the dollar sign ($) to be ignored, then enter the value as shown:
	`ignoreChar=*$`
	Suppose User2 is a member of the TESTGRP1, *TESTGRP2, and *TESTGRP$ profiles. If a LIST function is run for User2, then the following profiles are listed:
	`TESTGRP1, TESTGRP2, TESTGRP`

processFailedXML	This property is used by the Top Secret Reconcile Users to Internal LDAP scheduled task and determines whether the LDAP gateway will attempt to parse any failed XML entries. Default value: `true`
isStreamingUsers	This property is used by the Top Secret Reconcile Users to Internal LDAP scheduled task. If you set the value of this property to `true,` the LDAP gateway will process the CFILE data from the mainframe. If you set the value of this property to `false,` the LDAP gateway will not process any CFILE data. Default value: `true`

revokePsuspendUsers	Use this property to specify whether users with the PSUSPEND attribute should be flagged as revoked when parsing a LIST USER result message.
	■ Set `true` as the value if you want the user to be disabled in Oracle Identity Manager as the outcome of a LIST USER reconciliation operation.
	■ Set `false` as the value if you want the PSUSPEND attribute to not factor into the user's Oracle Identity Manager Status setting as the outcome of a LIST USER reconciliation operation.
	For example:
	`# REVOKE OIM USERS WITH PSUSPEND`
	`revokePsuspendUsers=true`

secretKeyValue	This property contains the custom encryption key. This key should match the secretKey value used by the mainframe agents. See Appendix B, "AES 128 User Key Definition and Usage" for more information on using this property.

Table 2–6 (Cont.) Properties in the tops.properties File

Property	Description
includeData	This property is used when retrieving a list of all users on the Top Secret system. If you set the value of this property to true, for each ACID in TSS, the LDAP gateway will return both the ACID and the user data. If you set the value of this property to false, for each ACID in TSS, the LDAP gateway will only the ACID. Default value: `false`
resumeOnReset	This property is used when resetting a user's password. If you set the value of this property to true, the user will be enabled during a reset password operation. If you set the value of this property to false, the user will not be enabled during a reset password operation. Default value: `true`
trimOmvsUid	This property is used with the omvsUid attribute. If you set the value of this property to true, the LDAP gateway will trim leading zeros, "0", from the omvsUid value. If you set the value of this property to false, the LDAP gateway will not trim any leading zeroes from the omvsUid value. Default value: `true`
trimNum	This property is used with the trimOmvsUid property and specifies the number of leading zeroes to trim from a user's omvsUid attribute. Default value: `2`
newOmvsUidAttr	This property specifies the new name to use for the omvsUid property. Default value: `OmvsUidEmplNumber`
usePwdComplexLength	This property is used to control the length of passwords. If you set the value of this property to true, the LDAP gateway will use the properties file password length settings. If you set the value of this property to false, the LDAP gateway will use the standard password length. Default value: `true`
idMinLength	This property specifies the minimum ACID length in characters. Default value: `1`
idMaxLength	This property specifies the maximum ACID length in characters. Default value: `8`
pwdMinLength	This property specifies the minimum password length for an ACID. Default value: `1`
pwdMaxLength	This property specifies the maximum password length for an ACID. Default value: `8`
minDays	This password specifies the minimum number of days that must pass before a password can be changed. Default value: `0`

Table 2–6 (Cont.) Properties in the tops.properties File

Property	Description
mainframeCodePage	This property specifies the mainframe code page in use on the mainframe. Default value: `CP857`
luMulti	This property is used with LU6.2 attributes. If you set the value of this property to true, the LDAP gateway will process LU6.2 attributes as multi-valued attributes. If you set the value of this property to false, the LDAP gateway will process LU6.2 attributes as single-valued attributes. Default value: `true`
luMultiSep	This property is used with LU6.2 attributes and specifies the separator character used for multi-valued attributes. Default value: |
type isencrypted timeout authretries requestorId CPF CPF-WAIT	These properties are no longer used in Oracle installations. Do not modify their values.

3. Save and close the tops.properties file.

4. From the *LDAP_INSTALL_DIR*/dist/idfserver.jar file, extract the beans.xml file and then open it in an editor.

5. In the beans.xml file, set values for the LDAP Gateway user credentials as follows:

   You use the beans.xml file to store the credentials of the account used by Oracle Identity Manager to connect to the LDAP Gateway. You also enter these credentials as parameters of the IT resource. During provisioning and reconciliation, the credentials passed through the IT resource are authenticated against the credentials stored in the beans.xml file. The LDAP Gateway exchanges data with the connector only after this authentication succeeds.

   You enter the credentials of the LDAP Gateway user in the following lines of the beans.xml file:

   ```
   <property name="adminUserDN" value="cn=idfTopsAdmin,dc=tops,dc=com"/>
   <property name="adminUserPassword" value="idfTopsPwd"/>
   ```

   In the first line, replace **`cn=idfTopsAdmin,dc=tops,dc=com`** with the value that you set for the idfPrincipalDn parameter of the IT resource. In the second line, replace the sample value **`idfTopsPwd`** with the encrypted version of the password that you set for the idfPrincipalPwd parameter of the IT resource. Table 2–2, " IT Resource Parameters" describes both parameters. If you want to encrypt the password before you enter it in the beans.xml file, then:

Note: It is optional to encrypt the password that you set in the beans.xml file. However, it is recommended that you encrypt the password for security reasons.

You must enter the unencrypted password as the value of the idfPrincipalPwd IT resource parameter. This is regardless of whether you enter the encrypted password in the beans.xml file.

---

a. 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
```

b. 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\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
```

c. Save the changes made to the propertyEncrypt.bat or propertyEncrypt.sh script.

d. Run the script.

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

e. In the beans.xml file, search for the following string:

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

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

For example:

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

6. In the beans.xml file, specify the port used for communication between the LDAP Gateway and the mainframe logical partition (LPAR) that you use for the connector installation

As shown in the following line, the default value of the port property is `5389`. You can change this default value to any port of your choice.

The port number should match the value that you specify for the idfServerPort IT resource parameter.

```
<property name="port" value="6389"/>
```

7. To enable logging for the LDAP Gateway:

   a. Copy the log4j JAR file from the application server directory in which it is placed to the *LDAP_INSTALL_DIR*/lib directory.

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

   c. Enter a log level as the value of the log4j.rootLogger variable. For example:

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

   See Also: Section 2.4.4, "Enabling Logging" for more information

   d. Save and close the file.

   When you use the connector, the following log file is generated in the *LDAP_INSTALL_DIR*/logs directory:

   idfserver.log.0: This is the main LDAP Gateway operations log file.

8. To configure the SSL in the LDAP Gateway:

   a. Edit the /ldapgateway/idfserver.jar beans.xml directory for the following:

   ```
   <bean id="sslChannelFactory"
   class="com.identityforge.idfserver.nio.ssl.SSLChannelFactory">
   <constructor-arg><value>false</value></constructor-arg>
   <constructor-arg><value>./conf/idf.jks</value></constructor-arg>
   <constructor-arg><value>abc123</value></constructor-arg>
   <constructor-arg><value>false</value></constructor-arg>
   </bean>
   ```

   The first argument indicates we are not in client mode.

   Note: Do not change this argument.

   The second argument is the path to the keystore. Either change this path to your keystore or add your certificate to this keystore.

   The third argument is the keystore password that you used to generate your keystore.

   The fourth argument indicates whether the keystore password is encrypted. Use `false` for plain-text passwords, and `true` for encrypted passwords.

   b. Edit a listener using the SSLChannelFactory for only "port", which is the only item you can change in the listener:

   ```
   <bean id="sslListener" class="com.identityforge.idfserver.nio.Listener">
   constructor-arg><ref bean="bus"/></constructor-arg>
   <constructor-arg><ref bean="sslChannelFactory"/></constructor-arg>
   <property name="admin"><value>false</value></property>
   <property name="config"><value>./conf/listener.xml</value></property>
   ```

```
<property name="port" value="7389"/>
<property name="threadName" value="SSLLDAPListener"/>
</bean>
```

c. Add the listener to the server by uncommenting the following line:

```
<bean id="server" class="com.identityforge.idfserver.Server">
<property name="tasks">
<list>
<ref bean="bus"/>
<ref bean="decoder"/>
<ref bean="listener"/>
<!-- <ref bean="sslListener"/>  ? <!- added here ->
<ref bean="client"/>
<ref bean="protocol"/>
<ref bean="encoder"/>
<ref bean="output"/>
</list>
</property>
<property name="nexus" ref="nexus"/>
<property name="logPath" value="../logs/idfserver.log"/>
</bean>
```

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

10. To configure the LDAP Gateway for the application server that Oracle Identity Manager is running on:

    a. In a text editor, open the run script from the *LDAP_INSTALL_DIR*/bin directory. This run script is used to start and stop the LDAP gateway.

       If using a Windows system, open the run.bat file.

       If using a UNIX system, open the run.sh file.

    b. In the run script, you will need to update certain sections (see the run script comments for more details):

       (i) Update the environment variables to reflect the actual location of the application server directories

```
rem ****************************************************
rem ******* UPDATE THE FOLLOWING CLASSPATHS *************
rem ****************************************************

set JAVA_HOME=C:\software\Java\jdk1.6.0_20
set APPSERVER_HOME=C:\jboss
set OIM_HOME=C:\oracle\9.0.3\xellerate
set OIM_CLIENT_HOME=C:\oracle\9.0.3\client\xlclient
```

       (ii) Uncomment the lines related to the application server libraries that you are using.

       (iii) Update the application server library classpaths to reflect the actual location of the directories on your system.

       (iv) Uncomment the STARTUP command for the application server that you are using.

    c. 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 script 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
```

11. Save and close the run script.

Starting and Stopping the LDAP Gateway on UNIX

To start the LDAP Gateway on UNIX, run the following command:

bin>./run.sh

When the LDAP Gateway has started, the `LDAP Gateway VERSION_NUMBER Started` message is recorded in the LDAP_INSTALL_DIR/bin/nohup.out log file. For more information on logging, see Section 2.4.4, "Enabling Logging."

To stop the LDAP Gateway on UNIX, run the following command:

bin>./stop_idf.sh

Starting and Stopping the LDAP Gateway on Microsoft Windows

To start the LDAP Gateway on Microsoft Windows, run the run.bat file.

When the LDAP Gateway has started, the `LDAP Gateway VERSION_NUMBER Started` message is recorded in the idfserver.log.

To stop the LDAP Gateway on Microsoft Windows, close the command window in which the gateway is running.

3 Connector Deployment on the Mainframe

You deploy the Reconciliation Agent and Provisioning Agent on the mainframe. These agents communicate with the LDAP Gateway during connector operations.

The following section summarizes the procedure to deploy the Reconciliation Agent and Provisioning Agent:

Section 3.7, "Summary of the Deployment Procedure"

The following sections describe each deployment step in detail:

- Section 3.1, "Reviewing Deployment Requirements"
- Section 3.2, "Deploying the Reconciliation Agent and Provisioning Agent"
- Section 3.3, "Editing the Mainframe Batch Job Files"
- Section 3.4, "Installing or Integrating the Reconciliation Agent Exit"
- Section 3.5, "Set APF Authorization for Pioneer and Voyager"
- Section 3.6, "Creating a CA Top Secret Account for Connector Operations"
- Section 3.7, "Summary of the Deployment Procedure"
- Section 3.8, "Configuring the Started Tasks"
- Section 3.9, "Pioneer and Voyager Operator Commands"
- Section 3.10, "Starting Up and Shutting Down the Reconciliation Agent"

See the following section if you want to remove the Reconciliation Agent exit:

Section 3.11, "Removing the Exit"

3.1 Reviewing Deployment Requirements

The following is a summary of the deployment requirements:

- The Reconciliation Agent and Provisioning Agent need a CA Top Secret ACID. This ACID that has administrative privileges to run functions such as Create, Change, List, and Replace.

> **Note:** **APF Authorization:** The executable code for Pioneer, Voyager and the TSSINSTX exit must execute from a APF authorized library. The APF authorization is required to make calls to the CA Top-Secret Security SubSystem. The APF authorized library can be in the z/OS Link List or a Steplib.

- The Reconciliation agent uses ECSA storage to store Top-Secret events. These events are the primary Top-Secret type commands which are 32 bytes in length. The subpool (231), which is allocated above the 16M line, requires from 200K to 7500K of ECSA memory for storage of CA Top Secret events. The range of the number of messages store range from 6400 to 240000.
- The Reconciliation Agent is fed by using a modified CA Top Secret exit. The exit (TSSINSTX) runs as part of CA Top Secret in the IBM z/OS operating system environment. Various exits points within the exit capture various CA Top-Secret events, primarily the Top-Secret commands to create, change, modify an ACID as well as the permits for various resources. If the exit fails, then the command fails and returns an error message. If the subpool allocated is full, for example; the LDAP is down, messages will be lost without risk to the Operating System. Maintaining a specific password format is an example of the objective for which you use custom exits, such as the one used by the Reconciliation Agent. The Reconciliation Agent exit is engineered to be the last exit called in sequence. This allows existing exits to function normally.

3.2 Deploying the Reconciliation Agent and Provisioning Agent

To deploy the Reconciliation Agent and Provisioning Agent (whether a new installation or an update, the process is the same):

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

   Table 3–1 lists the JES2 XMIT files that are included in the Mainframe_TS.zip file.

Table 3–1 JES2 XMIT Files

File Name	Description
linklib.xmi	Executable library for all modules.
parmlib.xmi	PROG member for dynamically authorizing IDF.LINKLIB.
proclib.xmi	Contains all the STC (Started Task Procedures).
clistlib.xmi	Contains LDAP search Rexx clists.
jcllib.xmi	Contains product installation JCL.
rexxlib.xmi	Contains the system Rexx library to be added to the AXR member.

2. Log in to the TSO environment of the mainframe. In this guide, a 3270 terminal emulator program called QWS3270P is used.
3. Perform the following steps either from the TSO Ready prompt or by using ISPF Option #6 using a TN3270 or TN3270E emulator:

   > **Note:** Each file must be uploaded in binary format without any file conversion. You can also use FTP to upload the files.

   a. Use the IND$FILE command to upload each of the files to the mainframe. The QWS3270P program has an upload option that will enter a properly formatted command. The upload options are:

      File Conversion: Nothing selected (No ASCII/EBCDIC translation and no CRLF).

Host Type: TSO selected.

Record Format: Default selected.

Sizes: LRECL and **BLKSIZE** are left blank.

Note: Alternatively, the record format can be "Fixed" with the LRECL set to "80" and the BLKSIZE set to "3120".

---

b. When prompted for dataset names, use the information given in Table 3–2.

Table 3–2 File name on the Client Machine and on the Mainframe Host

Filename on Client Machine	Recommended File name on Mainframe Host
linklib.xmi	LINKLIB.XMIT
proclib.xmi	PROCLIB.XMIT
parmlib.xmi	PARMLIB.XMIT
jcllib.xmi	JCLLIB.XMIT
clistlib.xmi	CLISTLIB.XMIT
rexxlib.xmi	REXXLIB.XMIT

4. Use the RECEIVE command to extract the files or Partition Datasets (PDS) in each XMIT file.

For each file, enter the following command:

```
receive inda('filename')
```

For example, to extract the LINKLIB.XMIT file, enter the following command:

```
receive inda('linklib.xmit')
```

Note: The mainframe is case insensitive. You can enter linklib.xmit or LINKLIB.XMIT.

When prompted to enter restore parameters or 'DELETE' or 'END' +", enter the following:

```
dataset('prefix.XMIT library name')
```

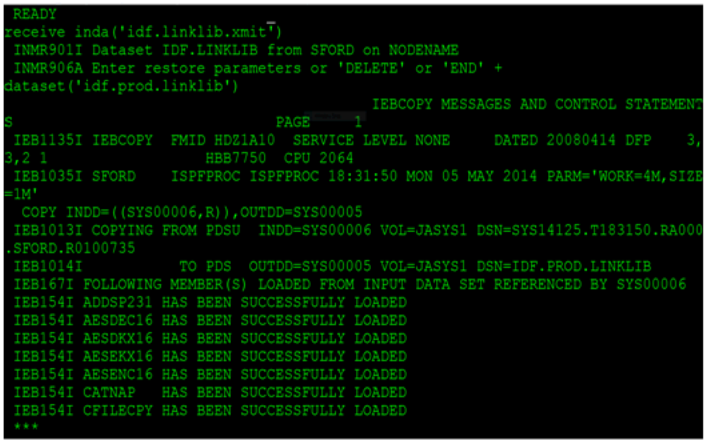
Use single quotes to specify a user name on the system as the prefix of the library. If you do not use single quotes, then the PDS will be created with a prefix of the user name with which you logged in.

Table 3–3 lists XMIT file names and corresponding sample PDS names.

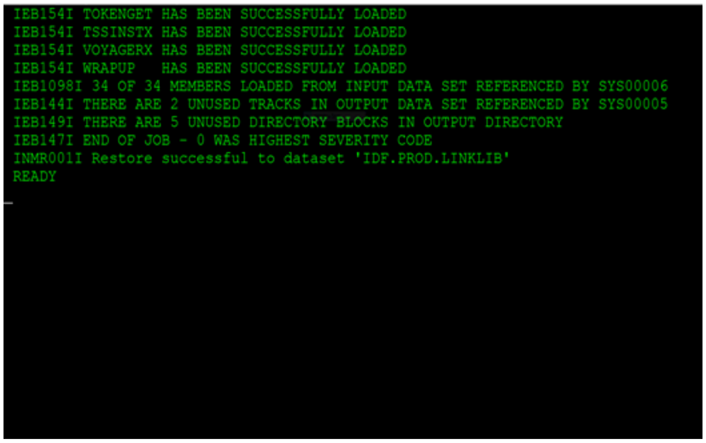
Table 3–3 XMIT File Names and PDS Names

XMIT file name on Mainframe Host	Recommended PDS name on Mainframe Host
LINKLIB.XMIT	IDF.LINKLIB
PROCLIB.XMIT	IDF.PROCLIB
PARMLIB.XMIT	IDF.PARMLIB
JCLLIB.XMIT	IDF.JCLLIB
CLISTLIB.XMIT	IDF.CLISTLIB
REXXLIB.XMIT	IDF.REXXLIB

5. The following screen images show the output from a TSO RECEIVE command where the "IDF.PROD.LINKLIB" dataset is entered at the prompt.



```
 READY
receive inda('idf.linklib.xmit')
 INMR901I Dataset IDF.LINKLIB from SFORD on NODENAME
 INMR906A Enter restore parameters or 'DELETE' or 'END' +
dataset('idf.prod.linklib')
                                     IEBCOPY MESSAGES AND CONTROL STATEMENT
S                              PAGE     1
 IEB1135I IEBCOPY  FMID HDZ1A10  SERVICE LEVEL NONE     DATED 20080414 DFP    3,
3,2 1                  HBB7750  CPU 2064
 IEB1035I SFORD    ISPFPROC ISPFPROC 18:31:50 MON 05 MAY 2014 PARM='WORK=4M,SIZE
=1M'
  COPY INDD=((SYS00006,R)),OUTDD=SYS00005
 IEB1013I COPYING FROM PDSU  INDD=SYS00006 VOL=JASYS1 DSN=SYS14125.T183150.RA000
.SFORD.R0100735
 IEB1014I           TO PDS  OUTDD=SYS00005 VOL=JASYS1 DSN=IDF.PROD.LINKLIB
 IEB167I FOLLOWING MEMBER(S) LOADED FROM INPUT DATA SET REFERENCED BY SYS00006
 IEB154I ADDSP231 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESDEC16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESDKX16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESEKX16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I AESENC16 HAS BEEN SUCCESSFULLY LOADED
 IEB154I CATNAP   HAS BEEN SUCCESSFULLY LOADED
 IEB154I CFILECPY HAS BEEN SUCCESSFULLY LOADED
 ***
```



```
 IEB154I TOKENGET HAS BEEN SUCCESSFULLY LOADED
 IEB154I TSSINSTX HAS BEEN SUCCESSFULLY LOADED
 IEB154I VOYAGERX HAS BEEN SUCCESSFULLY LOADED
 IEB154I WRAPUP   HAS BEEN SUCCESSFULLY LOADED
 IEB1098I 34 OF 34 MEMBERS LOADED FROM INPUT DATA SET REFERENCED BY SYS00006
 IEB144I THERE ARE 2 UNUSED TRACKS IN OUTPUT DATA SET REFERENCED BY SYS00005
 IEB149I THERE ARE 5 UNUSED DIRECTORY BLOCKS IN OUTPUT DIRECTORY
 IEB147I END OF JOB - 0 WAS HIGHEST SEVERITY CODE
 INMR001I Restore successful to dataset 'IDF.PROD.LINKLIB'
 READY
```

Note: The IDF.LINKLIB, once RECEIVED, can be either a STEPLIB or added to the environment's existing Linklist. This library must be APF authorized.

The following is the list of required authorization for REXXCLST (REXXC) and IDCALIAS (IDCAMSC):

- Both jobs must have access to the BATCH facility.
- Both jobs need access to UPDATE the dataset PIONEER.ALIAS.LSTOUT.
- Both jobs need access to UPDATE the dataset PIONEER.RECON.FILE.
- Both jobs need access to UPDATE the Master Catalog (that is ability to create/delete an alias for an ID).
- Both jobs need access to UPDATE the User-Catalog.

3.3 Editing the Mainframe Batch Job Files

The PDS IDF.JCLLIB file contains the CREATDSN, IEBCOPYL, IEBCOPYP, IEBCPYRP, and LOADDSN members, which must be edited to change file names, volsers, and job names to match your installation specifications. For each batch job, you must modify the job card to meet your installation specifications. The examples shown are non-SMS, these files can be SMS managed also.

1. Use the Data Set List Utility (ISPF option 3.4) to view the members in the PDS. To search for a PDS, enter the dataset name (or prefix) in the "Dsname Level" field.
2. Place an **E** (for Edit) to the left of the IDF.JCLLIB PDS.
3. Press **Enter** to edit the members in the PDS.
4. Place the cursor to the left of the member that you wish to edit.

Table 3–4 lists the JCLLIB member names and the corresponding description.

Table 3–4 JCLLIB members and their description

Member Name	Description
CREATDSN	Creates Pioneer and Voyager datasets.
CREATEXP	Creates EXPORTIN dataset for CFILE imports and output file for CFILECPYs and CONV2XML programs.
IDCAMSC	Input into LOADDSN step, this member is the JCL for IDCAMS alias functions.
LOADDSN	Loads INJCLR - jobstream for ALIAS support and loads RECONJCL.
IEBCOPYL	Copies TSSINSTX and IDFCACHE modules to the CA Top-Secret load library.
IEBCOPYP	Copies PROG01 to installation Parmlib.
KEYMODR	JCL stream to AMASZAP the encryption key, so the user can create their own encryption key.
PSAMCTL1/2	Pioneer Sample control file members
VSAMCTL1/2	Voyager Sample control file members
TSSCFILEV	CFILE execute stream for RECFM=VB CFILE.
TSSCFLEF	CFILE execute stream for RECFM=FB CFILE.
IEBCPYPR	Copies the STC procedures and other procedures used by the connector to the target system procedure library.
IEBCPYRX	Copies the connector Rexx clists to the target system libraries.
REXXCL	Used in LOADDSN to create a dataset skeleton for Pioneer.

The CREATDSN member is an IEFBR14 file creation stream that builds the files required for Pioneer and Voyager. For more information on each of the Pioneer and Voyager DDs see table Table 3–5 and Table 3–6.

Table 3–5 Pioneer DDs and their corresponding CREATDSN DD entries

Pioneer DD	CREATDSN DD

RECONJCL	//INDD1 DD DSN=PIONEER.RECON.LIBRARY,
	// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
	// UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG),
	// VOL=SER=XXXXXX

RECONOUT	//INDD2 DD DSN=PIONEER.RECON.FILE,
	// DCB=(DSORG=PS,RECFM=FB,LRECL=90,BLKSIZE=27000),
	// UNIT=SYSDA,SPACE=(CYL,50),DISP=(NEW,CATLG),
	// VOL=SER=XXXXXX

INJCLR	//INDD3 DD DSN=PIONEER.INJCL.LIBRARY,
	// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
	// UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG),
	// VOL=SER=XXXXXX

Table 3–5 (Cont.) Pioneer DDs and their corresponding CREATDSN DD entries

Pioneer DD	CREATDSN DD

LISTINR	//INDD4 DD DSN=PIONEER.ALIAS.LSTOUT,
	// DCB=(DSORG=PS,RECFM=VBA,LRECL=133,BLKSIZE=26300),
	// UNIT=SYSDA,SPACE=(CYL,5),DISP=(NEW,CATLG),
	// VOL=SER=XXXXXX

PARMFLE	//INDD6 DD DSN=PIONEER.ORACLE.CTLFLE,
	// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
	// UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG),
	// VOL=SER=XXXXXX

SYSTSPRT	//INDD7 DD DSN=PIONEER.REXXOUT.FILE,
	// DCB=(DSORG=PS,RECFM=FB,LRECL=121,BLKSIZE=27951),
	// UNIT=SYSDA,SPACE=(CYL,80),DISP=(NEW,CATLG),
	// VOL=SER=XXXXXX

SYSEXEC	//INDD8 DD DSN=PIONEER.REXX.CLISTS,
	// DCB=(DSORG=PO,RECFM=FB,LRECL=80,BLKSIZE=0),
	// UNIT=SYSDA,SPACE=(CYL,(5,5,1)),DISP=(NEW,CATLG),
	// VOL=SER=XXXXXX

Table 3–6 Voyager DDs and their corresponding CREATDSN DD entries

Voyager DD	CREATDSN DD

CACHESAV	//INDD7 DD DSN=VOYAGER.CACHESAV,
	// DCB=(DSORG=PS,RECFM=FB,LRECL=32,BLKSIZE=32000),
	// UNIT=SYSDA,SPACE=(CYL,10),DISP=(NEW,CATLG),
	// VOL=SER=??????

PARMFLE	//INDD9 DD DSN=VOYAGER.CONTROL.FILE,
	// DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80),
	// UNIT=SYSDA,SPACE=(TRK,1),DISP=(NEW,CATLG),
	// VOL=SER=??????

To update the CREATDSN member perform the following steps:

1. Modify the jobcard information (usually the first three lines of the batch file) to meet your installation specifications.
2. For each dataset name (DSN), "PIONEER" is used as the high-level qualifier (HLQ) for PIONEER files. "VOYAGER" is the HLQ used for VOYAGER files. You must change the HLQ for each DSN to meet your individual installation standards.
3. For each DSN, change the VOL=SER= field to point to the installation dasd volumes.
4. Submit the job and review the output. Successful return code (RC) is 0000.

The LOADDSN member loads the files created by CREATDSN to the defined load area.

Table 3–7 lists the LOADDSN steps and the corresponding file contents.

Table 3–7 LOADDSN steps and file contents loaded into Pioneer Datasets

LOADDSN Step	File Contents

Step #1	//STEP1 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(REXXCL),DISP=SHR
	//SYSUT2 DD DSN=PIONEER.RECON.LIBRARY,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

Step #2	//STEP2 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(ALIASLST),DISP=SHR
	//SYSUT2 DD DSN=PIONEER.INJCL.LIBRARY,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

Step #3	//STEP3 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(PSAMPLE),DISP=SHR
	//SYSUT2 DD DSN=PIONEER.CONTROL.FILE,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

Step #4	//STEP4 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(VSAMPLE),DISP=SHR
	//SYSUT2 DD DSN=VOYAGER.CONTROL.FILE,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

1. Modify the jobcard information to meet your installation standards.
2. For each DSN, "PIONEER" is the HLQ for PIONEER files, and "VOYAGER" is the HLQ for VOYAGER files. You are encouraged to change the HLQ to meet you individual installation standards.
3. For each DSN, edit the **SYSUT1** value to define the member to be loaded.
4. For each DSN, edit the **SYSUT2** value to define the sequential or flat file into which the member will be loaded.
5. Submit the job and review the output. Successful RC is 0000.

   The IEBCOPYL member copies the Top Secret exit and caching module (TSSINSTX and LOGCACHE) into the installation Top Secret Load library.

   Table 3–8 lists the IEBCOPYL variables and the corresponding sample value.

Table 3–8 IEBCOPYL Variables and Sample Values

IEBCOPYL Variable	Sample Value

Jobcard Information	//IEBCOPYL JOB SYSTEMS,MSGLEVEL=(1,1),
	// MSGCLASS=X,CLASS=A,PRTY=8,
	// NOTIFY=&SYSUID,REGION=4096K

INDD	DSN=IDF.PROD.LINKLIB
OUTDD	DSN=YOUR.LPALIB

Note: If your host mainframe has the TSSINSTX exit already in place, then it is your responsibility to integrate the exit. The TSSINSTX exit is loaded through the Top-Secret STC (TSS) or by command.

1. Modify the jobcard information to meet your installation standards.
2. Review and modify the INDD DSN to meet your installation standards.
3. Review and modify the OUTDD DSN to match the LPALIB in your installation.
4. Submit the job and review the output. Successful RC is 0000.

The IEBCOPYP member is an IEBCOPY file copy stream that copies a PROG member to an installation-defined parameter library.

Table 3–9 lists the IEBCOPYP variables and the corresponding sample values.

Table 3–9 IEBCOPYP Variables and Sample Values

IEBCOPYP Variable	Sample Value

Jobcard Information	//IEBCOPYP JOB SYSTEMS,MSGLEVEL=(1,1),
	// MSGCLASS=X,CLASS=A,PRTY=8,
	// NOTIFY=&SYSUID,REGION=4096K

INDD1	DSN=IDF.PROD.PARMLIB
OUTDD1	DSN=YOUR.PARMLIB

1. Modify the jobcard information to meet your installation standards.
2. Review and modify the INDD1 DSN to meet your installation standards.
3. Review and modify the OUTDD1 DSN to match the destination installation parameter library name (Parmlib) for the PROG member. The member PROGID sets APF authorization dynamically for IDF.LINKLIB. This can be added to an existing PROGxx member, if desired.
4. Submit the job and review the output. Successful RC is 0000

The IEBCPYPR member is an IEBCOPY file copy stream for the STC procedures and other procedures used by the product. PIONEER, VOYAGER, STARTUP and WRAPUP are Started Tasks (STC) procedures. The STARTUP and WRAPUP procedures allocate the subpool (231) cache (STARTUP) and delete the subpool (231) cache (WRAPUP) for Voyager. Startup must be run prior to Voyager to allocate the subpool (231) area used by VOYAGER. WRAPUP is to be executed after VOYAGER completes processing to free the subpool (231) area allocated by STARTUP and utilized by VOYAGER. See Section 3.1, "Reviewing Deployment Requirements" for further information.

Table 3–10 lists the IEBCPYPR variables and the corresponding sample values.

Table 3–10 IEBCPYPR Variables and Sample Values

IEBCPYPR Variable	Sample Value

Jobcard Information	//IEBCPYPR JOB SYSTEMS,MSGLEVEL=(1,1),
	// MSGCLASS=X,CLASS=A,PRTY=8,
	// NOTIFY=&SYSUID,REGION=4096K

INDD2	DSN=IDF.PROD.PROCLIB
OUTDD2	DSN=YOUR.HLQ.PROCLIB

1. Modify the jobcard information to meet your installation standards.
2. Review and modify the INDD2 DSN to meet your installation standards.

3. Review and modify the OUTDD2 DSN to match the installation procedure library name.
4. Submit the job and review the output. Successful RC is 0000.

Note: Files should not be shared in a SYSPLEX. Each Pioneer and Voyager must have their own set of files.

Table 3–11 CREATEXP (Optional CFILE) Variables and Values

CREATEXP Variable	Below Values as Shipped
//INDD1	DD DSN=YOURHLQ.CFILE.FILE,DCB=(DSORG=PS,RECFM=(<FB | VB>). This DD is only for customers who do not have a CFILE. It can be created as a RECFM=FB or RECFM=VB.
//INDD2	DD DSN=YOURHLQ.CFILE.OUT,DCB=(DSORG=PS,RECFM=FB,LRECL=320,BLKSIZE=0),UNIT=your-UNIT-name,SPACE=(CYL,???),DISP=(NEW,CATLG), this file is required whether the CFILE is RECFM=FB or RECFM=VB.
//INDD3	DD DSN=YOURHLQ.EXPORTIN.FILE,DCB=(DSORG=PS,RECFM=FB,LRECL=320,BLKSIZE=0), UNIT=your-UNIT-name,SPACE=(CYL,???),DISP=(NEW,CATLG), this file is required whether the CFILE is RECFM=FB or RECFM=VB.

1. Modify the jobcard information to meet your installation standards.
2. Review and modify the INDD1,2,3 to meet your installation standards.
3. Submit the job and review the output. Successful RC is 0000.

Note: Files should not be shared in a SYSPLEX. Each Pioneer and Voyager must have their own set of files.

3.4 Installing or Integrating the Reconciliation Agent Exit

After copying TSSINSTX and LOGCACHE to the installation CA Top-Secret Load Library (using the IEBCOPYL job stream), the Reconciliation Top-Secret exit has to be activated. If the destination Load Library is a Linklist, then an IPL is required to complete installation or integration of the Reconciliation Agent exit.

To allow the LDAP Gateway to fully capture events, the Reconciliation Agent and its exit must be installed on each LPAR that shares the authentication repository.

The following are the guidelines on using 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.
- The exit must be active and the subpool that contains TSS events must be active. If the exit is not active or if the subpool is not activated (by executing STARTUP), then CA 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 CA 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 CA 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.

The procedure that you must perform depends on whether or not other exits have already been installed:

- See Section 3.4.1, "Installing the Reconciliation Agent Exit" if there are no other exits installed on the mainframe.
- See Section 3.4.2, "Integrating the Reconciliation Agent Exit" if there are other exits installed on the mainframe.

3.4.1 Installing the Reconciliation Agent Exit

> **Note:** Perform the procedure described in this section only if there are no other exits installed on the mainframe. See Section 3.4.2, "Integrating the Reconciliation Agent Exit" if there are other exits installed on the mainframe.

To install the Reconciliation Agent exit:

1. Use the IEBCOPYL job stream to copy the TSSINSTX exit to the CA Top-Secret Load Library.
2. Perform an IPL on IBM z/OS.
3. To activate the exit code, perform any one of the following steps:
   - Run the following command from the IBM z/OS operator's console:

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

   - Modify the parmlib member (for example, TSSPARM0) of CA Top Secret by changing `EXIT(OFF)` to `EXIT(ON)`. After you change the parameter, run the `P TSS` z/OS command and then run the `S TSS` command.

   > **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.

Verifying the Exit

To verify that the exit loaded successfully, run the following command:

- From z/OS master console

  ```
  F TSS,MODIFY,STATUS
  ```

- From TSO

```
    TSS MODIFY STATUS
```

Deactivating the Exit

To deactivate the exit, run the following command:

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

3.4.2 Integrating the Reconciliation Agent Exit

> **Note:** Perform the procedure described in this section only if there are other exits installed on the mainframe. See Section 3.4.1, "Installing the Reconciliation Agent Exit" if there are no other exits installed on the mainframe.

If one or more third-party modules have been installed with the CA Top Secret (TSSINSTX) exit, then integration is required. This integration can be accomplished through code modification of either the Reconciliation Agent exit or the third-party exit. This should be done by qualified personnel well versed in MVS Assembler Language. If Oracle/IDF source is required for integration then an SR must be opened up with Oracle Support. This will then be reviewed.

3.5 Set APF Authorization for Pioneer and Voyager

The executable code (IBM z/OS loadlibs) of Pioneer and Voyager must be APF authorized. This can be achieved by running a dynamic set command (T PROD=ID) or by placing the installation loadlib containing Pioneer and Voyager in the IBM z/OS link list.

> **Note:**
>
> IBM® provides the PROGxx parmlib member as an alternative to IEAAPFxx, which allows you to update the APF list dynamically and specify an unlimited number of APF-authorized libraries. IBM suggests that you use PROGxx to specify the APF list (regardless of whether you plan to take advantage of the dynamic update capability). The system will process IEAAPFxx and PROGxx if both parameters are specified. If you decide to use PROGxx only, remove APF=xx system parameters from IEASYSxx and IEASYS00.

3.6 Creating a CA Top Secret Account for Connector Operations

The Reconciliation Agent and Provisioning Agent require a CA Top Secret ACID to which the permissions required for connector operations are applied. The following is an example of the commands to be run:

> **Note:** In these sample steps, VOYAGER and PIONEER are ACIDs. 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. The installation may have more or less restrictions depending on the overall security policy of the installation.

For the Reconciliation Agent:

```
CREATE(VOYAGER) TYPE(USER) NAME('VOYAGER ACID') PASSWORD(NOPW,0) FAC(STC)
ADD(VOYAGER) GROUP(OMVSGRP)
ADD(VOYAGER) DFLTGRP(OMVSGRP)
ADD(VOYAGER) GID(1)
PERMIT(VOYAGER) DSNAME(yourhlq.CACHESAV) ACCESS(UPDATE
PERMIT(VOYAGER) DSNAME(yourhlq.CONTROL.FILE) ACCESS(READ)
```

For the Provisioning Agent:

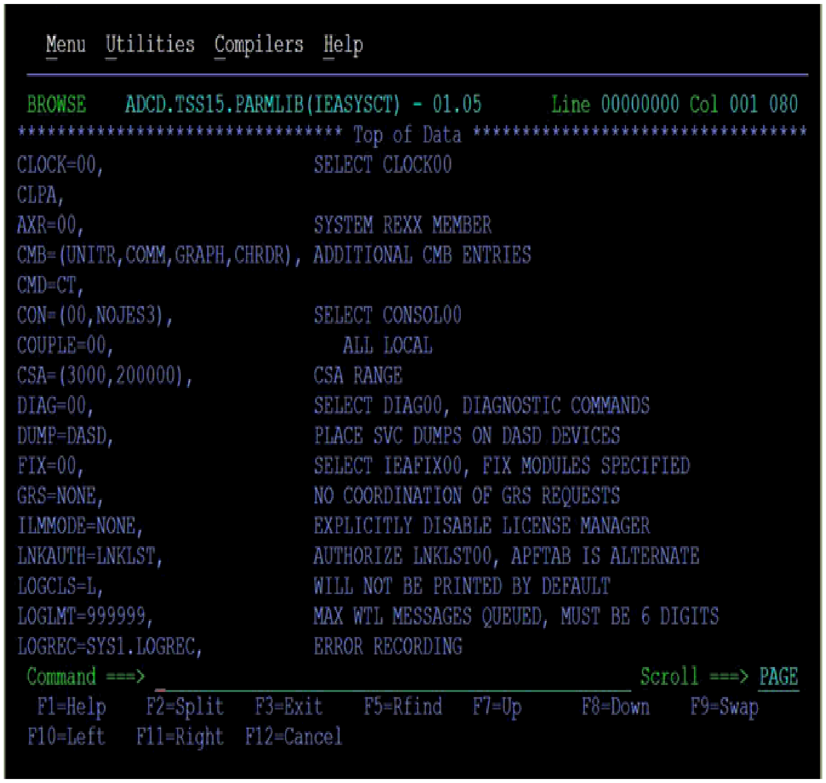
> **Note:** The Provisioning Agent is a TYPE(SCA) CA Top Secret full function Admin ID.

```
CREATE(PIONEER) TYPE(SCA) NAME('PIONVGR') PASSWORD(NOPW) FACILITY(BATCH,STC)
ADD(PIONEER) UID(0) GROUP(OMVSGRP) DFLTGRP(OMVSGRP) HOME(/) OMVSPGM(/BIN/SH)
ADDTO(STC) PROCNAME(PIONEER) ACID(PIONEER)
PERMIT(PIONEER) IBMFAC(BPX.*) ACCESS(READ)
PERMIT(PIONEER) IBMFAC(IRR.RADMIN.*) ACCESS(READ)
PERMIT(PIONEER) DSNAME(yourhlq.CONTROL.FILE) ACCESS(READ)
PERMIT(PIONEER) DSNAME(yourhlq.INJCL.LIBRARY) ACCESS(READ)
PERMIT(PIONEER) DSNAME(yourhlq.IDCAMS.LSTOUT) ACCESS(UPDATE)
PERMIT(PIONEER) DSNAME(yourhlq.RECON.LIBRARY) ACCESS(READ)
PERMIT(PIONEER) DSNAME(yourhlq.RECON.FILE) ACCESS(UPDATE)
PERMIT(PIONEER) DSNAME(yourhlq.EXPORT.FILE) ACCESS(UPDATE)
ADMIN(PIONEER) DATA(ALL)
ADMIN(PIONEER) ACID(ALL)
ADMIN(PIONEER) MISC2(ALL)
ADMIN(PIONEER) MISC8(ALL)
ADMIN(PIONEER) MISC9(ALL)
ADMIN(PIONEER) FAC(ALL)
```

> **Note:** The preceding Top-Secret authorities and permissions are a starting point, each Top-Secret environment is different in regards to access.
>
> Pioneer needs access to OMVS because of the TCPIP socket usage. This is normal for any Socket Server or Client. The ACCESS(UPDATE) on the above datasets is required for Pioneer to read and then clear (delete) the records in the files.

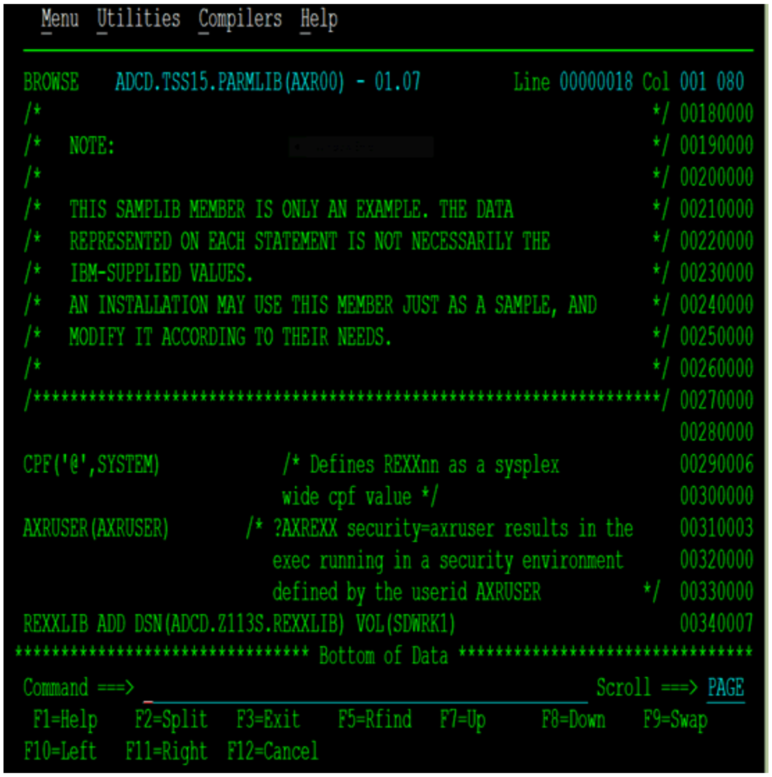
Support for LONG_FDTNAME

To extract the long **FDTNAMES**, Pioneer and Voyager use IBM's System Rexx product. The following screenshot of **sys1.parmlib(ieasysct)** shows the requirement of this product:



```
BROWSE    ADCD.TSS15.PARMLIB(IEASYSCT) - 01.05       Line 00000000 Col 001 080
******************************** Top of Data *********************************
CLOCK=00,                     SELECT CLOCK00
CLPA,
AXR=00,                       SYSTEM REXX MEMBER
CMB=(UNITR,COMM,GRAPH,CHRDR), ADDITIONAL CMB ENTRIES
CMD=CT,
CON=(00,NOJES3),              SELECT CONSOL00
COUPLE=00,                       ALL LOCAL
CSA=(3000,200000),            CSA RANGE
DIAG=00,                      SELECT DIAG00, DIAGNOSTIC COMMANDS
DUMP=DASD,                    PLACE SVC DUMPS ON DASD DEVICES
FIX=00,                       SELECT IEAFIX00, FIX MODULES SPECIFIED
GRS=NONE,                     NO COORDINATION OF GRS REQUESTS
ILMMODE=NONE,                 EXPLICITLY DISABLE LICENSE MANAGER
LNKAUTH=LNKLST,               AUTHORIZE LNKLST00, APFTAB IS ALTERNATE
LOGCLS=L,                     WILL NOT BE PRINTED BY DEFAULT
LOGLMT=999999,                MAX WTL MESSAGES QUEUED, MUST BE 6 DIGITS
LOGREC=SYS1.LOGREC,           ERROR RECORDING
 Command ===> _                                              Scroll ===> PAGE
  F1=Help    F2=Split   F3=Exit    F5=Rfind   F7=Up      F8=Down    F9=Swap
 F10=Left   F11=Right  F12=Cancel
```

The following screenshot of **sys1.parmlib(AXR00)** shows the requirement of this product and lists the dataset DCB attributes:

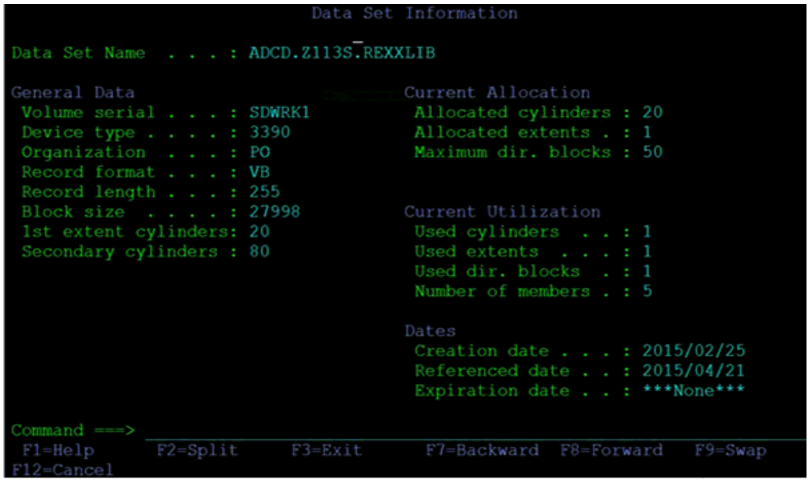


```
BROWSE    ADCD.TSS15.PARMLIB(AXR00) - 01.07         Line 00000018 Col 001 080
/*                                                                */ 00180000
/*   NOTE:                                                        */ 00190000
/*                                                                */ 00200000
/*   THIS SAMPLIB MEMBER IS ONLY AN EXAMPLE. THE DATA             */ 00210000
/*   REPRESENTED ON EACH STATEMENT IS NOT NECESSARILY THE         */ 00220000
/*   IBM-SUPPLIED VALUES.                                         */ 00230000
/*   AN INSTALLATION MAY USE THIS MEMBER JUST AS A SAMPLE, AND    */ 00240000
/*   MODIFY IT ACCORDING TO THEIR NEEDS.                          */ 00250000
/*                                                                */ 00260000
/*****************************************************************/ 00270000
                                                                     00280000
CPF('@',SYSTEM)             /* Defines REXXnn as a sysplex           00290006
                            wide cpf value */                        00300000
AXRUSER(AXRUSER)        /* ?AXREXX security=axruser results in the   00310003
                           exec running in a security environment    00320000
                           defined by the userid AXRUSER          */ 00330000
REXXLIB ADD DSN(ADCD.Z113S.REXXLIB) VOL(SDWRK1)                      00340007
****************************** Bottom of Data ******************************
Command ===> _                                             Scroll ===> PAGE
 F1=Help    F2=Split   F3=Exit    F5=Rfind   F7=Up      F8=Down    F9=Swap
F10=Left   F11=Right  F12=Cancel
```

```
CPF('@',SYSTEM) /* Defines REXXnn as a sysplex wide cpf value */
AXRUSER(AXRUSER) /* ?AXREXX security=axruser results in the exec running in a
```

```
security environment defined by the userid AXRUSER */

Note: As a reminder the active (SYS1.PARMLIB(IEASYSnn)) will need to contain:
AXR=  provides the name of the parmlib member in use (AXRxx) that specifies the
System REXX options,REXXLIB ADD DSN(ADCD.Z113S.REXXLIB) VOL(SDWRK1)
Refer to "IBM Knowledge Center" for more information about IEASYSxx parameters.
```



```
                        Data Set Information

Data Set Name  . . . : ADCD.Z113S.REXXLIB

General Data                         Current Allocation
 Volume serial . . . : SDWRK1         Allocated cylinders : 20
 Device type . . . . : 3390           Allocated extents . : 1
 Organization  . . . : PO             Maximum dir. blocks : 50
 Record format . . . : VB
 Record length . . . : 255
 Block size  . . . . : 27998         Current Utilization
 1st extent cylinders: 20             Used cylinders  . . : 1
 Secondary cylinders : 80             Used extents  . . . : 1
                                      Used dir. blocks  . : 1
                                      Number of members . : 5

                                     Dates
                                      Creation date . . . : 2015/02/25
                                      Referenced date . . : 2015/04/21
                                      Expiration date . . : ***None***

Command ===>
 F1=Help      F2=Split      F3=Exit       F7=Backward  F8=Forward    F9=Swap
F12=Cancel
```

The supplied REXXLIB is "sys1.saxrexec". This separates the RACF connector Rexx clists from the IBM Rexx clist.

IBM Shipped "AXRNN" STC Procedure:

```
//AXRNN    PROC
//EXEC PGM=AXRRXTSS
```

For the interface with IBM System Rexx:

1. Define AXRUSER

```
CREATE(AXRUSER) TYPE(USER) NAME('IBM-SYSTEM-REXX') PASSWORD(NOPW,0)
FAC(STC,BATCH)
ADD(AXRUSER) GROUP(OMVSGRP)
ADD(AXRUSER) DFLTGRP(OMVSGRP)
ADD(AXRUSER) GID(??)
ADD(STC) PROC(AXR) ACID(AXRUSER)
ADD(AXRUSER) HOME(/) OMVSPGM(/???????)
PERMIT(AXRUSER) SURROGAT(SYSREXX.AXRUSER) ACCESS(UPDATE)
```

2. Define AXRPSTRT

```
CREATE(AXRPSTRT) TYPE(USER) NAME('IBM-SYSTEM-REXX')
PASSWORD(NOPW,0)FAC(STC,BATCH)
ADD(AXRPSTRT) GROUP(OMVSGRP)
ADD(AXRPSTRT) DFLTGRP(OMVSGRP)
ADD(AXRPSTRT) GID(??)
ADD(STC) PROC(AXR) ACID(AXRPSTRT)
ADD(AXRPSTRT) HOME(/) OMVSPGM(/???????)
PERMIT(AXRUSER) SURROGAT(SYSREXX.AXRUSER) ACCESS(UPDATE)
```

3. IBM References for IBM System Rexx

```
MVS Programming: Authorized Assembler Services Guide
SA22-7608-17
```

Note: The installation where IBM System Rexx is being used may require more or different CA-Top Secret Security Definitions.

3.7 Summary of the Deployment Procedure

The following steps summarize the procedure to deploy the connector components on the target system:

1. Review and address the deployment requirements.
2. Extract the deployment files from the distribution .zip archive file.
3. Upload the files with an .xmi extension to the z/OS host.
4. Extract all mainframe XMIT files.
5. Modify the mainframe batch job files to match the settings of your target system installation.
6. Submit batch job streams to z/OS for execution and verify jobs completed successfully.
7. Activate and load the exits.
8. Create a CA Top Secret ACID for reconciliation and provisioning operations.
9. Add Pioneer/Voyager to the Facility Class Profiles (BPX and IRR).
10. Test the installation.

3.8 Configuring the Started Tasks

Configuring Pioneer

The JCL for the Pioneer Started Task (STC):

```
//PIONEER  EXEC PGM=PIONEERX,REGION=0M,TIME=1440
//JCLOUTP   DD SYSOUT=*
//PARMOUT   DD SYSOUT=*
//AUDTLOG   DD SYSOUT=*
//EXPTLOG   DD SYSOUT=*
//SYSOUT    DD SYSOUT=*
//DEBUGOUT  DD SYSOUT=*
//PARMFLE   DD DISP=SHR,DSN=PIONEER.CONTROL.FILE
//INJCLR    DD DISP=SHR,DSN=PIONEER.INJCL.LIBRARY
//LISTINR   DD DISP=SHR,DSN=PIONEER.ALIAS.LSTOUT,
//             DCB=(RECFM=VB,LRECL=137)
//RECONJCL  DD DISP=SHR,DSN=PIONEER.RECON.LIBRARY
//RECONOUT  DD DISP=SHR,DSN=PIONEER.RECON.FILE
//EXPORTIN  DD DISP=SHR,DSN=PIONEER.EXPORTIN.FILE
//SYSPUNCH DD SYSOUT=(*,INTRDR)
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=X
```

Pioneer Control File Parameter (DD:PARMFLE) Explanations

Table 3–12 lists the parameters of Pioneer control file.

Table 3–12 Pioneer Control File Parameters

Parameter	Sample Value	Description
TCPN=	TCPIP	Name of the TPCIP STC where Pioneer is executing. This is required for socket allocations. The limit is 8 characters.
ESIZE=	16	This option controls encryption during provisioning operations. Do not change the value of this parameter.
IPAD=	0.0.0.0	This is the only value supported.
PORT=	5198	The port used for communication between the LDAP Gateway and the Mainframe.
LPAR=	ZOS-112	The name of the LPAR defined for the Provisioning Agent. The name can be up to 20 characters long.
JWAIT=	010	Wait time from 001-999 seconds used for ALIAS submission.
RWAIT=	015	Wait time from 001-999 seconds used for Search Batch submissions.
POST_PROCESS_ALIAS=	`T or F`	T = True honor Alias requests. F = False do not honor Alias requests.
DEBUGOUT=	SYSOUT,CLASS(Y)	This parameter is used only when DEBUG=Y. Enter where to send DEBUG output and the JES2 output class that should be used.
DEBUG=	`Y or N`	Whether to turn on debugging. **Note:** Setting to Y generates a large amount of output.
IDLEMSG=	`Y or N`	"Y", show an IDLE message if Pioneer IDLE more than 60 minutes. "N" do not show.
SPIN_CLASS=	X is JES2 or JES3 class	Used with DEBUGOUT when a close is issued from modify command to Pioneer.
QUEUE_DSN=	???????????????	Temporary dataset that is used for batch search submissions. This dataset is "created" and "deleted" by Rexx Batch clists.
EXPORT_MON=	`NO or YES,REC=99999`	Used for CFILE XML EXPORT. "NO" for no EXPORTS, "YES,REC=01000", for EXPORTS and provide a status process message for every 1000 ACIDS.
AUDIT_LOG=	`Y or N`	Whether to turn on the audit log. AUDIT log will log LDAP and Pioneer processing requests. Output goes to AUDTLOG ddname of Pioneer.

Table 3–12 (Cont.) Pioneer Control File Parameters

Parameter	Sample Value	Description
LONG_FDTNAMES=	N or Y,DSN=??????????.????	Pioneer will process FDTNAMES that are long (over 255 bytes), where DSN= a temporary file that contains the listed output. The DSN is preallocated through the System Rexx clists.

Configuring Voyager

The following is the JCL for the Voyager STC (Started Task procedure):

```
//VOYAGER  PROC
//STEP1    EXEC PGM=VOYAGERX,REGION=0M,TIME=1440
//STEPLIB  DD DISP=SHR,DSN=IDF.LINKLIB <--- IF NOT IN LINKLIST
//CACHESAV DD DSN=VOYAGER.CACHESAV,DISP=SHR
//DEBUGOUT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//AUDTLOG  DD SYSOUT=*
//PARMOUT  DD SYSOUT=*
//PARMFLE  DD DISP=SHR,DSN=VOYAGER.CONTROL.FILE
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=X
//
```

Sample Voyager Control file:

```
* comment                                   this is a comment
TCPN=TCPIP                                  same parameter as Pioneer
IPAD=100.100.100.100                        LDAP address
PORT=5190                                   LDAP listening port
DEBUG=Y                                     DEBUGGING is on
ESIZE=16                                    AES128 encryption (key size in bytes)
VOYAGER_ID=TESTVOY1                         Voyager identifier used by LDAP
CACHE_DELAY=002
AUDIT_LOG=YES                               AUDIT log desired
CONNECT_MSGS=Y
MSGID01=YES,IDMV602E,02
CONNECT_RETRY=999
CONNECT_INTV=10
LONG_FDTNAMES=Y,DSN=<yourhlq.datasetname>
```

Voyager Control File Parameter (Configuring DD: PARMFLE) Explanations

Table 3–13 lists parameters of Voyager control file.

Table 3–13 Voyager Control File Parameters

Parameter	Sample Value	Description
*	Comment	
TCPN=	TCPIP	Name of the TPCIP STC where Voyager is executing. This is required for socket allocations. The maximum limit is 8 characters.
ESIZE=	16	This option controls encryption during reconciliation operations. Do not change the value of this parameter.

Table 3–13 (Cont.) Voyager Control File Parameters

Parameter	Sample Value	Description

IPAD=	`192.168.1.102`
	`myhost.work.com`
		IP address or hostname of the LDAP Gateway Host computer.

PORT=	`5190`	The outgoing connection port for the Reconciliation Agent to connect to the LDAP Gateway.
DEBUG=	`Y or N`	Whether to turn on debugging. **Note:** Setting to Y generates a large amount of output which goes to DEBUGOUT.
VOYAGER_ID=	`TESTVOY1`	An 8 character unique identifier that will be passed to the LDAP each time a reconciliation event occurs. The ID is used to identify the RACF database from which the reconciliation event was generated. If 8 LPARS, for example, are sharing 1 RACF database, all 8 LPARS must have the same VOYAGER_ID. The parameter value must match the file name of the corresponding VOYAGER_ID.properties located in the LDAP gateway installation.
CACHE_DELAY=	This must be a three-position numeric value. Examples: For no delay, use 000. This is adequate for most installations. For a two-second delay, use 002.	The number of seconds that Voyager waits between issuing a write socket to the LDAP gateway. This parameter is only used for installations running Oracle Identity Manager.
CONNECT_INTV=nn	Must be a two-digit value. Example 05 = Five Seconds	Number of seconds between retries to connect to LDAP if failure occurs. Use this parameter with the following entry: CONNECT_RETRY=
CONNECT_MSGS	`Y or N`	Display LDAP connect messages.
CONNECT_RETRY= nnn	Must be a three-digit value. 001-998: Indicates the number of retries 999: Indicates unlimited retries	Number of times to retry the LDAP Connection prior to AbEnd. Use this parameter with the following entry: CONNECT_INTV=
MSGID01=	`YES,IDMV602E,xx`	Displays the "LDAP cannot connect" message according to the number of times configured in this parameter.
AUDIT_LOG=	`Y or N`	This parameter logs LDAP and Voyager processing requests.
LONG_FDTNAMES=	`N or Y,DSN=??????????.???? Pioneer`	Used with FDTNAMES over 255 bytes. The DSN= segment is a temporary file that contains the listed output.

3.9 Pioneer and Voyager Operator Commands

The operator interface for Voyager and Pioneer, Polloper has been enhanced. Both STCs are single threaded. Table 3–14 lists the commands that are supported through the standard modify (F) interface.

Table 3–14 Pioneer and Voyager Operator Commands

Command	Description
F VOYAGER,SHUTDOWN	Shuts down Voyager
F VOYAGER,DEBUG=N	Turns off DEBUG
F VOYAGER,DEBUG=Y	Turns on DEBUG
F VOYAGER,STATUS	Voyager Status
F PIONEER,SHUTDOWN	Shuts down Pioneer
F PIONEER,STATUS	Pioneer Status
F PIONEER,DEBUG=Y	Turns DEBUG on
F PIONEER,DEBUG=N	Turns DEBUG off

3.10 Starting Up and Shutting Down the Reconciliation Agent

To start or stop the Voyager Agent:

1. VOYAGER as of 9.0.4.19 incorporates all the features of STARTUP and WRAPUP.
2. If you are starting a fresh run of Reconciliation Agent VOYAGER, first issue a "S STARTUP" to allocate the subpool (231) area used by VOYAGER.
3. Start the VOYAGER agent by running "S Voyager" from the console or SDSF in TSO.
4. To quiesce VOYAGER while leaving the subpool intact, stop VOYAGER by running "F VOYAGER.SHUTDOWN" from the console.
5. To quiesce VOYAGER and destroy the subpool, issue a "F VOYAGER,SHUTDOWN" and also issue a WRAPUP by running "S WRAPUP" from the console. User of WRAPUP will cause any messages stored in the subpool to be lost.
6. VOYAGER polls storage for events when they enter through TSO, BATCH or through Pioneer(LDAP) connection. VOYAGER reads all the available messages and processes them.

Note:

- Events detected by the Voyager Agent through the TSSINSTX installation exit are built into messages and passed to the LDAP Gateway.
- The messages are securely sent to the LDAP Gateway using AES128 encryption. If the LDAP Gateway is not running, then messages are held until the LDAP Gateway is returned to service and also secured in an AES-encrypted file on the mainframe. The messages are sent when the Gateway resumes running.

3.11 Removing the Exit

To remove the TSSINSTX exit, run the following command from the IBM z/OS operator's console:

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

4

Using the Connector

This chapter discusses the following topics:

4.1 Guidelines on Using the Connector

Apply the following guidelines while using the connector:

- The subpool and the LDAP Gateway must be started before starting the Reconciliation Agent. If the LDAP Gateway is not available when the Reconciliation Agent is started, then an error is generated with RETCODE=-01 and ERRORNO=61.
- The Top Secret connector LDAP gateway encrypts ASCII data transmitting the encrypted message to the mainframe. The mainframe decrypts this message, as the in bound message is in ASCII format, it is translated to EBCDIC for mainframe processing. 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. 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. (See bug 18268599 for related information)
- 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. Keep in mind these requirements when you create or modify target system accounts through provisioning operations on Oracle Identity Manager.

4.2 Scheduled Tasks for Lookup Field Synchronization

The following are the scheduled tasks for lookup field synchronization:

- Top Secret Find All Facilities
- Top Secret Find All Datasets
- Top Secret Find All Profiles
- Top Secret Find All Groups

These scheduled tasks populate lookup tables with facility, dataset, group, or profiles IDs that can be assigned during the user provisioning process. When you configure these scheduled tasks, they run at specified intervals and fetch a listing of all facility, dataset, group, or profiles IDs on the target system for reconciliation.

Table 4–1 describes the attributes of the scheduled task.

Table 4–1 Attributes of the Find All Facilities, Find All Datasets, Find All Profiles and Find All Groups Scheduled Tasks

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `TopSecretResource`
Resource Object	Enter the name of the resource object against which provisioning runs must be performed. Sample value: `OIMTopSecretResourceObject`
Lookup Code Name	Enter the name of the lookup code where OIM will store the results of the scheduled task. Sample value: `Lookup.profileNames` **Note:** The value supplied for the Lookup Code Name should match the value set in the properties of the Lookup Field in the corresponding Top Secret child table form.
Recon Type	Enter "Append" or "Replace". This attribute determines whether the values from the target system will be appended to the current lookup, or replace the existing values in the lookup. If set to `"Replace",` the existing lookup will be deleted. Sample value: `Replace`
R2	Enter whether the version of Oracle Identity Manager in use is 11.1.2.*x*. Sample value: `true`

4.3 Configuring the Sources Lookup Field

The Lookup.SourceNames lookup definition is created in Oracle Identity Manager when you deploy the connector and is used to add and remove a user's access to a source on the mainframe. This connector includes a scheduled task to automatically populate the lookup field used for storing Top Secret source IDs. Table 4.2 describes the properties of the Find All Sources scheduled task.

Note: The Find All Sources scheduled task does not query the target system for data. Instead, the scheduled task automatically populates the lookup field with "itResourceKey~sourceName" pairs based on the IT Resource and Find All Sources scheduled task property values.

Table 4–2 Attributes of the Find All Sources Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `TopSecretResource`
Resource Object	Enter the name of the resource object against which provisioning runs must be performed. Sample value: `OIMTopSecretResourceObject`
Sources List	Enter a comma-separated list of Top Secret sources. Sample value: `TSO,R5`
Lookup Code Name	Enter the name of the lookup code where Oracle Identity Manager will store the source entries. Sample value: `Lookup.SourceNames`
Recon Type	Enter "Append" or "Replace". This attribute determines whether "IT resource key~sourceName" pairs will be appended to the current lookup, or replace the existing values in the lookup. If set to "Replace", the existing lookup will be deleted. Sample value: `Replace`
R2	Enter whether the version of Oracle Identity Manager in use is 11.1.2.*x*. Sample value: `true`

However, you can also manually add additional values. To add additional sources for provisioning and reconciliation perform the following steps:

1. Log in to Oracle Identity Manager Design Console.
2. Expand **Administration** and then double-click **Lookup Definition.**
3. Search for the **Lookup.SourceNames** lookup definition.
4. Click **Add.**
5. In the Code Key column, enter the name of the source.
6. Enter the same value in the Decode column. The following is a sample entry: Code Key: `R5` Decode: `R5`
7. Click the Save icon.

4.4 Configuring Reconciliation

The CA Top Secret Advanced connector supports both incremental reconciliation (sometimes referred to as real-time reconciliation) and full reconciliation. This section discusses the following topics related to configuring reconciliation:

- Section 4.4.1, "Full Reconciliation"
- Section 4.4.2, "Reconciliation Scheduled Tasks"

4.4.1 Full Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager. After you deploy the connector, you must first perform full reconciliation.

When you run the Connector Installer, a scheduled job for user reconciliation (Top Secret Reconcile All Users) is automatically created in Oracle Identity Manager.

To perform full reconciliation, run the Top Secret Reconcile All Users scheduled job. See Section 4.4.2.1, "Top Secret Reconcile All Users" for more information.

4.4.2 Reconciliation Scheduled Tasks

When you run the Connector Installer, the following reconciliation scheduled tasks are automatically created in Oracle Identity Manager:

- Section 4.4.2.1, "Top Secret Reconcile All Users"
- Section 4.4.2.2, "Top Secret Reconcile Deleted Users to OIM"
- Section 4.4.2.3, "Top Secret Reconcile Users to Internal LDAP"
- Section 4.4.2.4, "Top Secret Reconcile All LDAP Users"

4.4.2.1 Top Secret Reconcile All Users

The Top Secret Reconcile All Users scheduled task is used to reconcile user data in the target resource (account management) mode of the connector. This scheduled task runs at specified intervals and fetches create or modify events on the target system for reconciliation.

Table 4–3 describes the attributes of the scheduled task.

Table 4–3 Attributes of the Top Secret Reconcile All Users Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `TopSecretResource`
Resource Object	Enter the name of the resource object against which reconciliation runs must be performed. Sample value: `OIMTopSecretResourceObject`
MultiValuedAttributes	Enter a comma-separated list of multivalued attributes that you want to reconcile. Do not include a space after each comma. Sample value: `profiles,sources,groupIds,facilities`
SingleValueAttributes	Enter a comma-separated list of single-valued attributes that you want to reconcile. Do not include a space after each comma. Do not include attributes already listed in the MultiValueAttributes field. Sample value: `uid,owner,defaultGroup,waddr1,tsoMaxSize` **Note**: By default, Oracle Identity Manager's design form only allows entering up to 150 characters in a text field. To increase this limit, change the value of the TSA_VALUE column in Oracle Identity Manager database.
UID Case	Enter either "upper" or "lower" for the case for the UID attribute value. Sample value: `upper`
UsersList	Enter a comma-separated list of UIDs that you want to reconcile from the target system. If this property is left blank, all users on the target system will be reconciled. Sample value: `userQA01,georgeb,marthaj,RST0354`
R2	Enter whether the version of Oracle Identity Manager in use is 11.1.2.*x*. Sample value: `true`

4.4.2.2 Top Secret Reconcile Deleted Users to OIM

The Top Secret Reconcile Deleted Users to OIM scheduled task is used to reconcile data about deleted users in the target resource (account management) mode of the connector.

When you configure this scheduled task, it runs at specified intervals and fetches a list of users on the target system. These user names are then compared with provisioned users in Oracle Identity Manager. Any user profiles that exist within Oracle Identity Manager, but not in the target system, are deleted from Oracle Identity Manager.

Table 4–4 describes the attributes of the scheduled task.

Table 4–4 Attributes of the Top Secret Reconcile Deleted Users to Oracle Identity Manager Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value:`TopSecretResource`
Resource Object	Enter the name of the resource object against which the delete reconciliation runs must be performed. Sample value: `OIMTopSecretResourceObject`
Recon Matching Rule Attributes	Enter a comma-separated list of attributes used in the matching rule. If the IT resource is used, enter "IT". Sample value: `UID,IT`

4.4.2.3 Top Secret Reconcile Users to Internal LDAP

The Top Secret Reconcile Users to Internal LDAP scheduled task is used to process the CFILE extract from the target system to the internal LDAP store. When you configure this scheduled task, it runs at specified intervals and fetches a list of users and their profiles on the target system. Each of these users is then reconciled to the internal LDAP store. No reconciliation to Oracle Identity Manager is performed.

Table 4–5 describes the attributes of the scheduled task.

Table 4–5 Attributes of the Top Secret Reconcile Users to Internal LDAP Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `TopSecretResource`
Domain OU	Enter the name of the internally-configured directory in the LDAP internal store where the contents of event changes will be stored. Sample value: `tops`

4.4.2.4 Top Secret Reconcile All LDAP Users

The Top Secret Reconcile All LDAP Users scheduled task is used to reconcile users from the internal LDAP store to Oracle Identity Manager. When you configure this scheduled task, it runs at specified intervals and fetches a list of users within the internal LDAP store and reconciles these users to Oracle Identity Manager.

Table 4–6 describes the attributes of the scheduled task.

Table 4–6 Attributes of the Top Secret Reconcile All LDAP Users Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `TopSecretResource`
Resource Object	Enter the name of the resource object against which the delete reconciliation runs must be performed. Sample value: `OIMTopSecretResourceObject`
Domain OU	Enter the name of the internally-configured directory in the LDAP internal store where the contents of event changes will be stored. Sample value: `tops`
MultiValuedAttributes	Enter a comma-separated list of multivalued attributes that you want to reconcile. Do not include a space after each comma. Sample value: `profiles,sources,facilities,groupIds`
SingleValueAttributes	Enter a comma-separated list of single-valued attributes that you want to reconcile. Do not include a space after each comma. Do not include attributes already listed in the MultiValueAttributes field. Sample value: `uid,owner,defaultGroup,waddr1,tsoMaxSize` **Note:** By default, Oracle Identity Manager's design form only allows entering up to 150 characters in a text field. To increase this limit, change the value of the TSA_VALUE column in the Oracle Identity Manager database.
LDAP Time Zone	Enter the time zone ID for the server on which the LDAP gateway is hosted. Sample value: `EST`
UID Case	Enter whether the user ID should be displayed in uppercase or lowercase. Sample value: `upper`

4.4.3 Configuring Filtered Reconciliation to Multiple Resource Objects

Some organizations use multiple resource objects to represent multiple user types in their system. The Resource Object property of the Top Secret Reconcile All Users scheduled task is used to specify the resource object used during reconciliation, and you can enter more than one resource object in the value of the Resource Object attribute. Further, you can include CA Top Secret attribute-value pairs to filter records for each resource object.

> **See Also:** Section 4.4.2.1, "Top Secret Reconcile All Users" for information about the Top Secret Reconcile All Users scheduled task

The following is a sample format of the value for the Resource Object attribute:

```
(ATTRIBUTE1:VALUE1)RESOURCE_OBJECT1,RESOURCE_OBJECT2
```

As shown by RESOURCE_OBJECT2 in the sample format, specifying a filter attribute is optional, but if more than one resource object is specified, you must specify a filter for each additional resource object. If you do not specify a filter attribute, then all records are reconciled to the first resource object in the list. Further, the filters are checked in order, so the resource object without a filter attribute should be included last in the list.

Filter attributes should be surrounded by parentheses.

Apply the following guidelines while specifying a value for the Resource Object attribute:

- The names of the resource objects must be the same as the names that you specified while creating the resource objects in the Oracle Identity Manager Design Console.
- The CA Top Secret attribute names must be the same as the names used in the LDAP Gateway configuration files.

  > **See Also:** Section 2.6, "Installing and Configuring the LDAP Gateway" 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() API call of the regex matcher is used rather than the matches() API call. This means that a substring matching rule can be specified in the pattern, rather than requiring the entire string matching rule.

  Further, substring matching is case-sensitive. A "(tso)" filter will not match a user with the user ID "TSOUSER1".

- Multiple values can be matched. Use a vertical bar (|) for a separator as shown in the following 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 Resource Object attribute:

```
(tsoProc:X)TSSR01,(instdata:value1|value2|value3)TopSecretResourceObject2,(tso)Top
SecretResourceObject24000,Resource
```

In this sample value:

- (tsoProc:X)TSSRO1 represents a user with X as the attribute value for the TSO Proc segment. Records that meet this criterion are reconciled with the TSSRO1 resource object.
- (instdata:value1|value2|value3)TopSecretResourceObject2 represents a user with value1, value2, or value3 as their INSTDATA attribute value. Records that meet this criterion are reconciled with the TopSecretResourceObject2 resource object.
- (tso)TopSecretResourceObject24000 represents a user with TSO privileges. A TSO attribute value is not specified. Records that meet this criterion are reconciled with the TopSecretResourceObject24000 resource object.
- All other records are reconciled with the resource object.

4.5 Configuring Account Status Reconciliation

> **Note:** This section describes an optional procedure. Perform this procedure only if you want reconciliation of user status changes on CA Top Secret.

When a user is disabled or enabled on the target system, the status of the user can be reconciled into Oracle Identity Manager. To configure reconciliation of user status changes made on CA Top Secret:

1. If using scheduled task reconciliation, in the Top Secret Reconcile All Users scheduled task, add the Status attribute to the SingleValueAttributes property list.
2. In the Design Console:

   See Also: *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for detailed information about the following steps

   - In the **OIMTopSecretResourceObject** resource object, create a reconciliation field to represent the Status attribute.
   - In the **OIMTopsProvisioningProcess** process definition, map the field for the Status field to the OIM_OBJECT_STATUS field.

     See Bug 6668844 in Chapter 7, "Known Issues and Workarounds" for information about a limitation related to the OIM_OBJECT_STATUS field.

4.6 Configuring Scheduled Tasks

This section describes the procedure to configure scheduled tasks. You can apply this procedure to configure the scheduled tasks for lookup field synchronization and reconciliation.

Table Table 4–7 lists the scheduled tasks that you must configure.

Table 4–7 Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
Top Secret Find All Groups	This scheduled task is used to synchronize the values of group lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see Section 4.2, "Scheduled Tasks for Lookup Field Synchronization."
TopSecret Find All Facilities	This scheduled task is used to synchronize the values of facilities lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see Section 4.2, "Scheduled Tasks for Lookup Field Synchronization."
Top Secret Find All Datasets	This scheduled task is used to synchronize the values of dataset lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see Section 4.2, "Scheduled Tasks for Lookup Field Synchronization."
Top Secret Find All Profiles	This scheduled task is used to synchronize the values of profiles lookup fields between Oracle Identity Manager and the target system. For information about this scheduled task and its attributes, see Section 4.2, "Scheduled Tasks for Lookup Field Synchronization."
Top Secret Find All Sources	This scheduled task is used to synchronize the values of source lookup fields in Oracle Identity Manager. For information about this scheduled task and its attributes, see Section 4.2, "Scheduled Tasks for Lookup Field Synchronization."
Top Secret Reconcile All Users	This scheduled task is used to fetch user data during target resource reconciliation. For information about this scheduled task and its attributes, see Section 4.4.2.1, "Top Secret Reconcile All Users."

Table 4–7 (Cont.) Scheduled Tasks for Lookup Field Synchronization and Reconciliation

Scheduled Task	Description
Top Secret Reconcile Deleted Users to OIM	This scheduled task is used to fetch data about deleted users during target resource reconciliation. During a reconciliation run, for each deleted user account on the target system, the Top Secret User resource is revoked for the corresponding OIM User. For information about this scheduled task and its attributes, see Section 4.4.2.2, "Top Secret Reconcile Deleted Users to OIM."
Top Secret Reconcile Users to Internal LDAP	This scheduled task is used to reconcile users from the target system to the internal LDAP store. For information about this scheduled task and its attributes, see Section 4.4.2.3, "Top Secret Reconcile Users to Internal LDAP."
Top Secret Reconcile All LDAP Users	This scheduled task is used to reconcile users from the internal LDAP store to Oracle Identity Manager. For information about this scheduled task and its attributes, see Section 4.4.2.4, "Top Secret Reconcile All LDAP Users."

To configure a scheduled task:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:

   - For Oracle Identity Manager release 11.1.1.*x:*

     a. Log in to the Oracle Identity System Administration.

     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.

     c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs.**

   - For Oracle Identity Manager release 11.1.2.*x*:

     a. Log in to Oracle Identity System Administration.

     b. In the left pane, under System Management, click **Scheduler.**

2. Search for and open the scheduled task as follows:

   a. In the Search field, enter the name of the scheduled job as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.

   b. In the search results table on the left pane, click the **scheduled job** in the Job Name column.

3. On the Job Details tab, you can modify the following parameters:

   - **Retries:** Enter an integer value in this field. This number represents the number of times the scheduler tries to start the job before assigning the Stopped status to the job.

   - **Schedule Type:** Depending on the frequency at which you want the job to run, select the appropriate schedule type.

   > **Note:** See Scheduled Tasks in *Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed information about schedule types.

   In addition to modifying the job details, you can enable or disable a job.

4. On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task.

Note:

- Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.
- Values (either default or user-defined) must be assigned to all the attributes. If even a single attribute value is left empty, then reconciliation is not performed.
- See "Reconciliation Scheduled Tasks" for the list of scheduled tasks and their attributes.

5. Click Apply to save the changes.

Note: The Stop Execution option is available in the Oracle Identity System Administration. You can use the Scheduler Status page to either start, stop, or reinitialize the scheduler.

4.7 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.1.*x*

Provisioning a resource for an OIM User involves using Oracle Identity Manager to create a target system account for the user.

When you install the connector on Oracle Identity Manager, the direct provisioning feature is automatically enabled. This means that the process form is enabled when you install the connector.

If you have configured the connector for request-based provisioning, then the process form is suppressed and the object form is displayed. In other words, direct provisioning is disabled when you configure the connector for request-based provisioning. If you want to revert to direct provisioning, then perform the steps described in Section 4.7.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager."

This following are types of provisioning operations:

- Direct provisioning
- Request-based provisioning
- Provisioning triggered by policy changes

See Also: See Managing Provisioning Tasks in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for information about the types of provisioning

This section discusses the following topics:

- Section 4.7.1, "Direct Provisioning"
- Section 4.7.2, "Request-Based Provisioning"
- Section 4.7.3, "Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager"

4.7.1 Direct Provisioning

To provision a resource by using the direct provisioning approach:

1. Log in to the Oracle Identity System Administration.
2. If you want to first create an OIM User and then provision a target system account, then:
   a. On the Welcome to Identity Administration page, in the Users region, click **Create User.**
   b. On the Create User page, enter values for the OIM User fields, and then click **Save.**
3. If you want to provision a target system account to an existing OIM User, then:
   a. On the Welcome to Identity Administration page, search for the OIM User by selecting **Users** from the list on the left pane.
   b. From the list of users displayed in the search results, select the OIM User. The user details page is displayed on the right pane.
4. On the user details page, click the **Resources** tab.
5. From the Action menu, select **Add Resource**. Alternatively, you can click the add resource icon with the plus (+) sign. The Provision Resource to User page is displayed in a new window.
6. On the Step 1: Select a Resource page, select **OIMTopSecretResourceObject** from the list and then click **Continue.**
7. On the Step 2: Verify Resource Selection page, click **Continue.**
8. On the Step 5: Provide Process Data for Top Secret Advanced Details page, enter the details of the account that you want to create on the target system and then click **Continue**.
9. On the Step 5: Provide Process Data for Top Secret Profile Membership Details page, search for and select a profile for the user on the target system and then click **Continue.**
10. On the Step 5: Provide Process Data for Top Secret Facility Membership Details page, search for and select a facility for the user on the target system and then click **Continue.**
11. On the Step 5: Provide Process Data for Top Secret Sources Membership Details page, enter a source for the user on the target system and then click **Continue.**
12. On the Step 5: Provide Process Data for Top Secret Dataset Membership Details page, search for and select a dataset for the user on the target system and then click **Continue.**
13. On the Step 6: Verify Process Data page, verify the data that you have provided and then click **Continue.**
14. Close the window displaying the "Provisioning has been initiated" message.
15. On the Resources tab, click **Refresh** to view the newly provisioned resource.

4.7.2 Request-Based Provisioning

A request-based provisioning operation involves both end users and approvers. Typically, these approvers are in the management chain of the requesters. The following sections discuss the steps to be performed by end users and approvers during a request-based provisioning operation:

> **Note:** The procedures described in these sections are built on an example in which the end user raises or creates a request for provisioning a target system account. This request is then approved by the approver.

- Section 4.7.2.1, "End User's Role in Request-Based Provisioning"
- Section 4.7.2.2, "Approver's Role in Request-Based Provisioning"

4.7.2.1 End User's Role in Request-Based Provisioning

The following steps are performed by the end user in a request-based provisioning operation:

> **See Also:** *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for detailed information about these steps

1. Log in to the Oracle Identity Self Service.
2. On the Welcome page, click **Advanced** in the upper-right corner of the page.
3. On the Welcome to Identity Administration page, click the **Administration** tab, and then click the **Requests** tab.
4. From the Actions menu on the left pane, select **Create Request.**

   The Select Request Template page is displayed.
5. From the Request Template list, select **Provision Resource** and click **Next.**
6. On the Select Users page, specify a search criterion in the fields to search for the user that you want to provision the resource, and then click **Search.** A list of users that match the search criterion you specify is displayed in the Available Users list.
7. From the **Available Users** list, select the user to whom you want to provision the account.

   If you want to create a provisioning request for more than one user, then from the **Available Users** list, select users to whom you want to provision the account.
8. Click **Move** or **Move All** to include your selection in the Selected Users list, and then click **Next.**
9. On the Select Resources page, click the arrow button next to the Resource Name field to display the list of all available resources.
10. From the Available Resources list, select **OIMTopSecretResourceObject**, move it to the Selected Resources list, and then click **Next.**
11. On the Resource Details page, enter details of the account that must be created on the target system, and then click **Next.**
12. On the Justification page, you can specify values for the following fields, and then click **Finish.**
    - Effective Date
    - Justification

    On the resulting page, a message confirming that your request has been sent successfully is displayed along with the Request ID.
13. If you click the Request ID, then the Request Details page is displayed.

14. To view details of the approval, on the Request Details page, click the **Request History** tab.

4.7.2.2 Approver's Role in Request-Based Provisioning

The following are steps performed by the approver in a request-based provisioning operation:

The following are steps that the approver can perform:

1. Log in to the Oracle Identity System Administration.
2. On the Welcome page, click **Self-Service** in the upper-right corner of the page.
3. On the Welcome to Identity Manager Self Service page, click the **Tasks** tab.
4. On the **Approvals** tab, in the first section, you can specify a search criterion for request task that is assigned to you.
5. From the search results table, select the row containing the request you want to approve, and then click **Approve Task.**

   A message confirming that the task was approved is displayed.

4.7.3 Switching Between Request-Based Provisioning and Direct Provisioning on Oracle Identity Manager

> **Note:** It is assumed that you have performed the procedure described in Section 2.5, "Configuring Oracle Identity Manager for Request-Based Provisioning."

If you want to switch from request-based provisioning to direct provisioning, then:

1. Log in to the Design Console.
2. Disable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition.**
   b. Search for and open the **OIMTopProvisioningProcess** process definition.
   c. Deselect the Auto Save Form check box.
   d. Click the Save icon.
3. If the Self Request Allowed feature is enabled, then:
   a. Expand **Resource Management**, and then double-click **Resource Objects.**
   b. Search for and open the **OIMTopSecretResourceObject** resource object.
   c. Deselect the **Self Request Allowed** check box.
   d. Click the Save icon.

If you want to switch from direct provisioning back to request-based provisioning, then:

1. Log in to the Design Console.
2. Enable the Auto Save Form feature as follows:
   a. Expand **Process Management**, and then double-click **Process Definition.**

   b. Search for and open the **OIMTopsProvisioningProcess** process definition.
   c. Select the **Auto Save Form** check box.
   d. Click the Save icon.

3. If you want to enable end users to raise requests for themselves, then:

   a. Expand **Resource Management**, and then double-click **Resource Objects**.
   b. Search for and open the **OIMTopSecretResourceObject** resource object.
   c. Select the Self Request Allowed check box.
   d. Click the Save icon.

4.8 Performing Provisioning Operations in Oracle Identity Manager Release 11.1.2 or Later

To perform provisioning operations in Oracle Identity Manager release 11.1.2 or later:

1. Log in to Oracle Identity Oracle Identity System Administration.
2. Create a user. See Managing Users in *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for more information about creating a user.
3. On the Account tab, click **Request Accounts.**
4. In the Catalog page, search for and add to cart the application instance created in Step 3, and then click **Checkout.**
5. Specify value for fields in the application form and then click **Ready to Submit.**
6. Click **Submit.**
7. If you want to provision entitlements, then:

   a. On the Entitlements tab, click **Request Entitlements.**
   b. In the Catalog page, search for and add to cart the entitlement, and then click **Checkout.**
   c. Click **Submit.**

5

Extending the Functionality of the Connector

This chapter discusses the following optional procedures that you can perform to extend the functionality of the connector for addressing your business requirements:

- Section 5.1, "Adding Custom Fields for Target Resource Reconciliation"
- Section 5.2, "Adding Custom Multivalued Fields for Reconciliation"
- Section 5.3, "Adding Custom Fields for Provisioning"
- Section 5.4, "Removing Attributes Mapped for Target Resource Reconciliation"
- Section 5.5, "Configuring the Connector for Provisioning to Multiple Installations of the Target System"
- Section 5.6, "Configuring the Generation of Single-Use Passwords for the Reset Password Operation"
- Section 5.7, "Initial LDAP Gateway Population and Full Reconciliation"
- Section 5.8, "Configuring Windows Service"
- Section 5.9, "Customizing Log File Locations"

5.1 Adding Custom Fields for Target Resource Reconciliation

Note: You must ensure that new attributes you add for reconciliation contain only string-format data. Binary attributes must not be brought into Oracle Identity Manager natively.

By default, the attributes listed in Table 1–4 are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

To add a custom field for reconciliation, you must first update the connector reconciliation component you are using, and then update Oracle Identity Manager. This section discusses the following topics:

- Section 5.1.1, "Adding Custom Fields for Full Reconciliation"
- Section 5.1.2, "Adding Custom Fields to Oracle Identity Manager"

5.1.1 Adding Custom Fields for Full Reconciliation

You can add custom fields for full reconciliation by specifying a value for the SingleValueAttributes attribute of the Top Secret Reconcile All Users scheduled task. See Section 4.4.1, "Full Reconciliation" for more information.

To add a custom field for scheduled task reconciliation:

1. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x:*
     a. Log in to the Oracle Identity System Administration.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
     c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs.**
   - For Oracle Identity Manager release 11.1.2.*x*:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click **Scheduler.**
2. Search for and open the **Top Secret Reconcile All Users** scheduled task as follows:
   a. In the left pane, in the Search field, enter `Top Secret Reconcile All Users` as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the scheduled job in the Job Name column.
3. Add the custom field to the list of attributes in the `SingleValueAttributes` scheduled task attribute.
4. Click **Apply.**

5.1.2 Adding Custom Fields to Oracle Identity Manager

After adding the custom field to the Top Secret Reconcile All users scheduled task (if using scheduled task reconciliation), you must add the custom field to the Oracle Identity Manager components.

To update Oracle Identity Manager with the custom field:

1. Log in to the Oracle Identity Manager Design Console.
2. Add the custom field to the list of reconciliation fields in the resource object as follows:
   a. Expand **Resource Management** and then double-click **Resource Objects.**
   b. Search for and open the **OIMTopSecretResourceObject** resource object.
   c. On the Object Reconciliation tab, click **Add Field.**
   d. In the Add Reconciliation Field dialog box, enter the details of the field.

      For example, if you are adding a Top Secret attribute called "Description", then enter `Description` in the Field Name field and select **String** from the Field Type list.
   e. Click **Save** and close the dialog box.

f. Click **Create Reconciliation Profile.** This copies changes made to the resource object into MDS.

g. Click **Save.**

3. Add the custom field on the process form as follows:

   a. Expand **Development Tools** and then double-click **Form Designer.**

   b. Search for and open the **UD_IDF_TOPS** process form.

   c. Click **Create New Version,** and then click **Add.**

   d. Enter the details of the field.

      For example, if you are adding the Description field, then enter `UD_IDF_TOPS_DESCRIPTION` in the Name field, and then enter the rest of the details of this field.

   e. Click **Save** and then click **Make Version Active.**

4. Create a reconciliation field mapping for the custom field in the provisioning process as follows:

   a. Expand **Process Management** and then double-click **Process Definition.**

   b. Search for and open the **OIMTopsProvisioningProcess** process definition.

   c. On the Reconciliation Field Mappings tab of the provisioning process, click **Add Field Map.**

   d. In the Add Reconciliation Field Mapping dialog box, from the Field Name field, select the value for the field that you want to add.

   e. For example, from the Field Name field, select **Description.**

   f. Double-click the **Process Data field**, and then select **UD_IDF_TOPS_DESCRIPTION.**

   g. Click **Save** and close the dialog box.

   h. Click **Save.**

5. If you are using Oracle Identity Manager release 11.1.2.*x*, then create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.4.1.2, "Creating a New UI Form" and Section 2.4.1.6, "Updating an Existing Application Instance with a New Form" for the procedures.

6. If you are adding a custom attribute or custom dataset, then set values for the _configAttrs_, _configDNames and _configDatasets_ properties in the tops.properties file. See Step 2 of Section 2.6, "Installing and Configuring the LDAP Gateway" for information about these properties.

5.2 Adding Custom Multivalued Fields for Reconciliation

To add a custom multivalued field to reconciliation, you must first update the IDF reconciliation component you are using, and then update Oracle Identity Manager.

- Section 5.2.1, "Adding Custom Multivalued Fields for Full Reconciliation"
- Section 5.2.2, "Adding Custom Multivalued Fields to Oracle Identity Manager"

5.2.1 Adding Custom Multivalued Fields for Full Reconciliation

You can add custom multivalued fields for full reconciliation by specifying a value for the multiValuedAttributes property of the Top Secret Reconcile All Users reconciliation scheduled task. See Section 4.4.2.1, "Top Secret Reconcile All Users" for more information.

To add a custom field for scheduled task reconciliation:

1. Log in to Oracle Identity System Administration.
2. Depending on the Oracle Identity Manager release you are using, perform one of the following steps:
   - For Oracle Identity Manager release 11.1.1.*x:*
     a. Log in to the Oracle Identity System Administration.
     b. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
     c. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs.**
   - For Oracle Identity Manager release 11.1.2.*x*:
     a. Log in to Oracle Identity System Administration.
     b. In the left pane, under System Management, click **Scheduler.**
3. Search for and open the **Top Secret Reconcile All Users** as follows:
   a. On the left pane, in the Search field, enter **Top Secret Reconcile All Users** as the search criterion. Alternatively, you can click **Advanced Search** and specify the search criterion.
   b. In the search results table on the left pane, click the **scheduled job** in the Job Name column.
4. Add the custom field to the list of attributes in the `MultiValuedAttributes property.`
5. Click **Apply.**

5.2.2 Adding Custom Multivalued Fields to Oracle Identity Manager

After adding the custom multivalued field to the Top Secret Reconcile All users scheduled task (if using scheduled task reconciliation), you must add the custom multivalued field to the Oracle Identity Manager components.

To update Oracle Identity Manager with the multivalued field:

1. Log in to the Oracle Identity Manager Design Console.
2. Create a form for the multivalued field as follows:
   a. Expand **Development Tools** and double-click **Form Designer.**
   b. Create a form by specifying a table name and description, and then click **Save.**
   c. Click **Add** and enter the details of the field.
   d. Click **Save** and then click **Make Version Active.** Figure 5–1 shows the multivalued field added on a new form.

Figure 5–1 Multivalued Field Added on a New Form

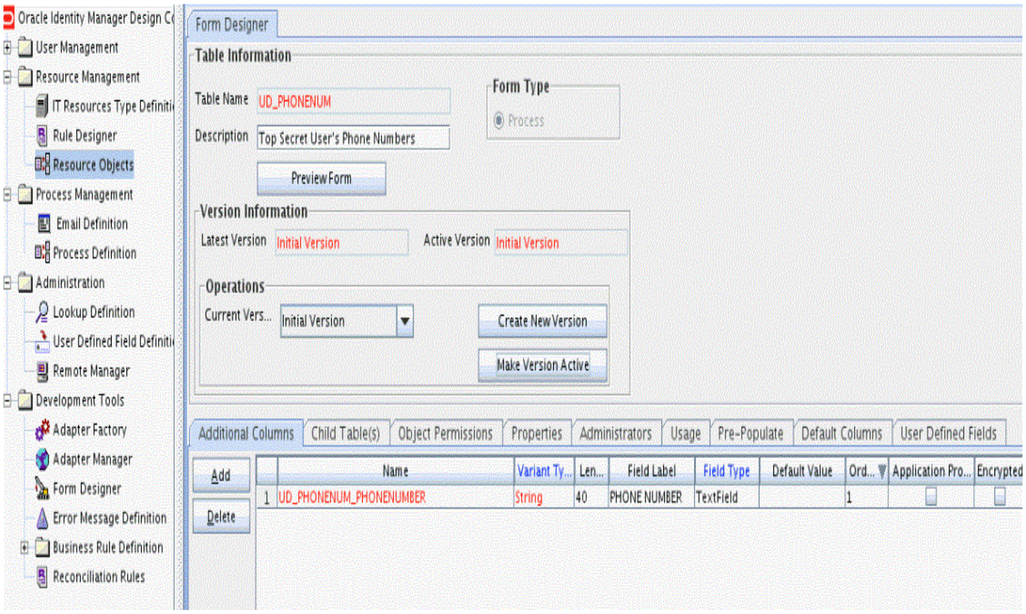


Table Information

Table Name: UD_PHONENUM

Description: Top Secret User's Phone Numbers

Form Type: ● Process

Version Information

Latest Version: Initial Version

Active Version: Initial Version

Operations

Current Vers...: Initial Version

	Name	Variant Ty...	Len...	Field Label	Field Type	Default Value	Ord...	Application Pro...	Encrypted
1	UD_PHONENUM_PHONENUMBER	String	40	PHONE NUMBER	TextField		1	□	□

3. Add the form created for the multivalued field as a child form of the process form as follows:

   a. Search for and open the **UD_IDF_TOPS** process form.

   b. Click **Create New Version.**

   c. Click the **Child Table(s) tab.**

   d. Click **Assign.**

   e. In the Assign Child Tables dialog box, select the newly created child form, click the **right arrow,** and then click **OK.**

   f. Click **Save** and then click **Make Version Active.** Figure 5–2 shows the child form added to the process form.

Figure 5–2 Child Form Added to the Process Form

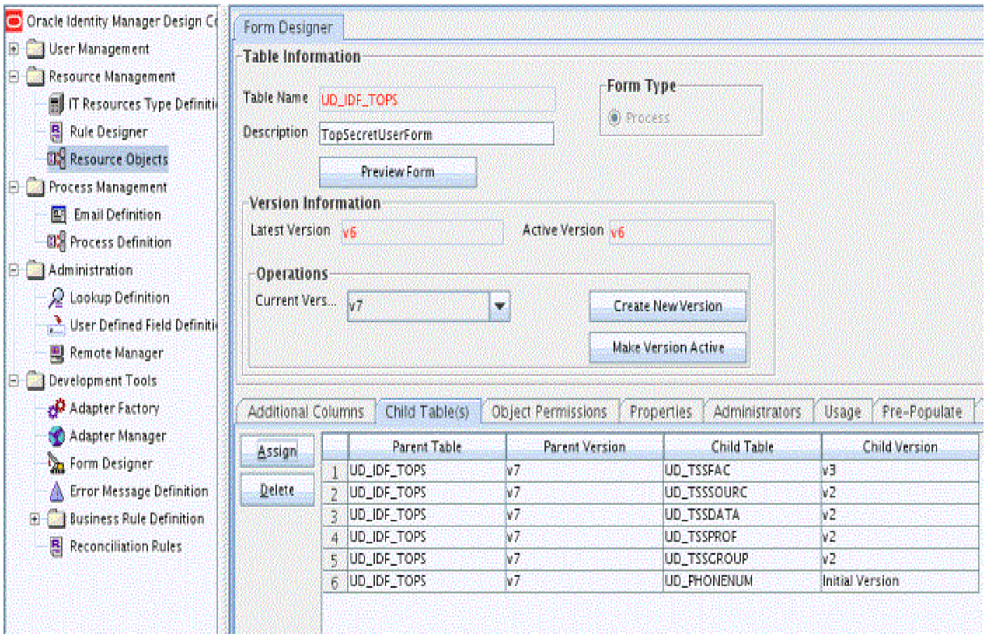


Table Information

Table Name: UD_IDF_TOPS

Description: TopSecretUserForm

Form Type: ● Process

Version Information

Latest Version: v6

Active Version: v6

Operations

Current Vers...: v7

	Parent Table	Parent Version	Child Table	Child Version
1	UD_IDF_TOPS	v7	UD_TSSFAC	v3
2	UD_IDF_TOPS	v7	UD_TSSSOURC	v2
3	UD_IDF_TOPS	v7	UD_TSSDATA	v2
4	UD_IDF_TOPS	v7	UD_TSSPROF	v2
5	UD_IDF_TOPS	v7	UD_TSSGROUP	v2
6	UD_IDF_TOPS	v7	UD_PHONENUM	Initial Version

4. Add the new multivalued field to the list of reconciliation fields in the resource object as follows:

   a. Expand **Resource Management** and then double-click **Resource Objects.**

   b. Search for and open the **OIMTopsResourceObject** resource object.

   c. On the Object Reconciliation tab, click **Add Field.**

   d. In the Add Reconciliation Field dialog box, enter the details of the field.

      For example, enter `phoneNumber` in the Field Name field and select **Multi-Valued Attribute** from the Field Type list.

   e. Click **Save** and close the dialog box.

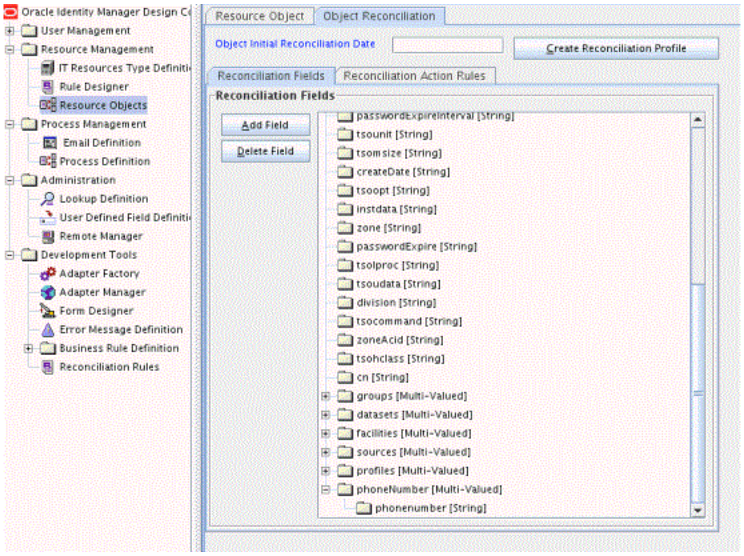
   f. Right-click the newly created field and select **Define Property Fields.**

   g. In the Add Reconciliation Fields dialog box, enter the details of the newly created field.

      For example, enter `phonenumber` in the Field Name field and select **String** from the Field Type list.

   h. Click **Save** and then close the dialog box. Figure 5–3 shows the new reconciliation field added in the resource object.

Figure 5–3 New Reconciliation Field Added in the Resource Object



i. Click **Create Reconciliation Profile.** This copies changes made to the resource object into MDS.

5. Create an entry for the field in the `AtMap.Tops` lookup definition, as follows:

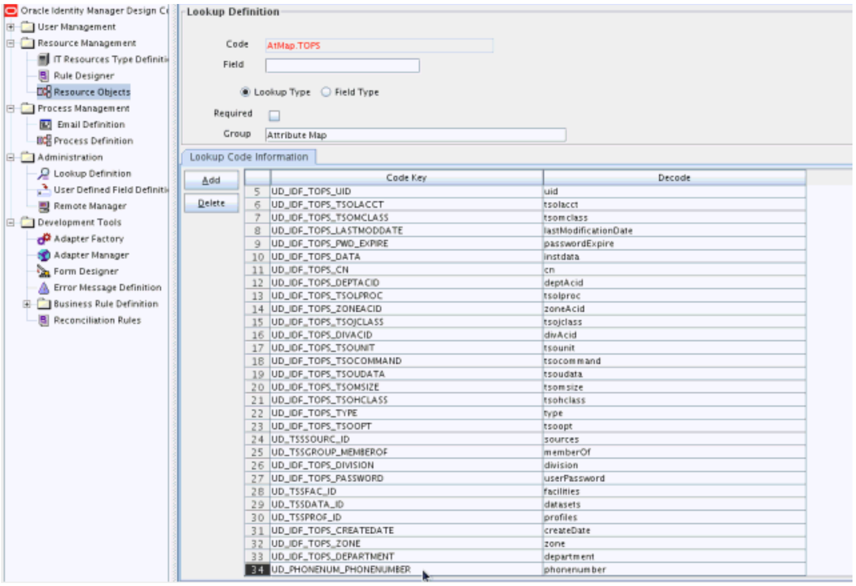
   a. Expand **Administration** and then double-click **Lookup Definition.**

   b. Search for the **AtMap.TOPS** lookup definition.

   c. Click **Add** and enter the Code Key and decode values for the field. The Code Key value is the name of the process form field that you created for the multivalued custom field in Step 3.d. The Decode value is the name of the target system field.

      For example, enter `UD_PHONENUM_PHONENUMBER` in the Code Key field and then enter `phonenumber` in the Decode field. Figure 5–4 shows the lookup code added to the lookup definition.

Figure 5–4 Entry Added in the Lookup Definition



Code: AtMap.TOPS

Field:

● Lookup Type ○ Field Type

Required □

Group: Attribute Map

	Code Key	Decode
5	UD_IDF_TOPS_UID	uid
6	UD_IDF_TOPS_TSOLACCT	tsolacct
7	UD_IDF_TOPS_TSOMCLASS	tsomclass
8	UD_IDF_TOPS_LASTMODDATE	lastModificationDate
9	UD_IDF_TOPS_PWD_EXPIRE	passwordExpire
10	UD_IDF_TOPS_DATA	instdata
11	UD_IDF_TOPS_CN	cn
12	UD_IDF_TOPS_DEPTACID	deptAcid
13	UD_IDF_TOPS_TSOLPROC	tsolproc
14	UD_IDF_TOPS_ZONEACID	zoneAcid
15	UD_IDF_TOPS_TSOJCLASS	tsojclass
16	UD_IDF_TOPS_DIVACID	divAcid
17	UD_IDF_TOPS_TSOUNIT	tsounit
18	UD_IDF_TOPS_TSOCOMMAND	tsocommand
19	UD_IDF_TOPS_TSOUDATA	tsoudata
20	UD_IDF_TOPS_TSOMSIZE	tsomsize
21	UD_IDF_TOPS_TSOHCLASS	tsohclass
22	UD_IDF_TOPS_TYPE	type
23	UD_IDF_TOPS_TSOOPT	tsoopt
24	UD_TSSSOURC_ID	sources
25	UD_TSSGROUP_MEMBEROF	memberOf
26	UD_IDF_TOPS_DIVISION	division
27	UD_IDF_TOPS_PASSWORD	userPassword
28	UD_TSSFAC_ID	facilities
29	UD_TSSDATA_ID	datasets
30	UD_TSSPROF_ID	profiles
31	UD_IDF_TOPS_CREATEDATE	createDate
32	UD_IDF_TOPS_ZONE	zone
33	UD_IDF_TOPS_DEPARTMENT	department
34	UD_PHONENUM_PHONENUMBER	phonenumber

d. Click **Save.**

6. Create a reconciliation field mapping for the new multivalued field as follows:

   a. Expand **Process Management** and then double-click **Process Definition.**

   b. Search for and open the **OIMTopsProvisioningProcess** process definition.

   c. On the Reconciliation Field Mappings tab of the provisioning process, click **Add Table Map.**

   d. In the Add Reconciliation Table Mapping dialog box, select the **field name** and table name from the list, click **Save,** and then close the dialog box.

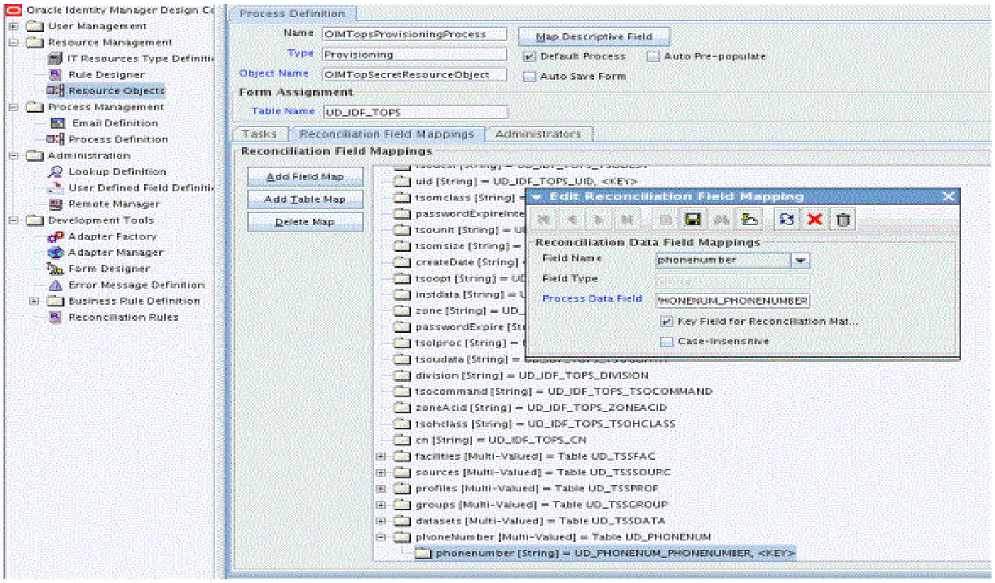
   e. Right-click the newly created field and select **Define Property Field Map.**

   f. In the Field Name field, select the value for the field that you want to add.

   g. Double-click the **Process Data** field, and then select **UD_PHONENUM_PHONENUMBER.**

   h. Select **Key Field** for Reconciliation Field Matching and click **Save.** Figure 5–5 shows the new reconciliation field mapped to a process data field in the process definition.

Figure 5–5 New Reconciliation Field Mapped to a Process Data Field



Name: OIMTopsProvisioningProcess

Type: Provisioning

Object Name: OIMTopSecretResourceObject

☑ Default Process □ Auto Pre-populate

□ Auto Save Form

Form Assignment

Table Name: UD_IDF_TOPS

Reconciliation Field Mappings

- uid [String] = UD_IDF_TOPS_UID, <KEY>
- tsomclass [String] =
- passwordExpireInte
- tsounit [String] = UI
- tsomsize [String] =
- createDate [String]
- tsoopt [String] = UD
- instdata [String] = U
- zone [String] = UD_
- passwordExpire [Str
- tsolproc [String] =
- tsoudata [String] =
- division [String] = UD_IDF_TOPS_DIVISION
- tsocommand [String] = UD_IDF_TOPS_TSOCOMMAND
- zoneAcid [String] = UD_IDF_TOPS_ZONEACID
- tsohclass [String] = UD_IDF_TOPS_TSOHCLASS
- cn [String] = UD_IDF_TOPS_CN
- facilities [Multi-Valued] = Table UD_TSSFAC
- sources [Multi-Valued] = Table UD_TSSSOURC
- profiles [Multi-Valued] = Table UD_TSSPROF
- groups [Multi-Valued] = Table UD_TSSGROUP
- datasets [Multi-Valued] = Table UD_TSSDATA
- phoneNumber [Multi-Valued] = Table UD_PHONENUM
  - phonenumber [String] = UD_PHONENUM_PHONENUMBER, <KEY>

Reconciliation Data Field Mappings

Field Name: phonenumber

Field Type: String

Process Data Field: HONENUM_PHONENUMBER

☑ Key Field for Reconciliation Mat...

□ Case-Insensitive

5.3 Adding Custom Fields for Provisioning

By default, the attributes listed in Table 1–4 are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

The connector does not support the use of custom attributes in CREATE USER operations that is, TSS CREATE. Instead, custom attribute modifications should be sent in an MODIFY USER operation that is, TSS ADDTO/REPLACE/REMOVE after the user has been provisioned a resource.

To add a new attribute for provisioning:

> **See Also:** *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for detailed information about these steps

1. Log in to the Oracle Identity Manager Design Console.
2. Add the new attribute on the process form as follows:

   If you have added the field on the process form by performing Step 4 of Section 5.1.2, "Adding Custom Fields to Oracle Identity Manager," then you need not add the field again. If you have not added the field, then:

   a. Expand **Development Tools.**

   b. Double-click **Form Designer.**

   c. Search for and open the **UD_IDF_TOPS** process form.

   d. Click **Create New Version,** and then click **Add.**

   e. Enter the details of the attribute.

      For example, if you are adding the Description field, enter **UD_IDF_TOPS_DESCRIPTION** in the Name field, and then enter the rest of the details of this field.

   f. Click **Save** and then click **Make Version Active.**

> **Note:** OMVS and NETVIEW attributes must not be added to the AtMap.TOPS lookup definition as they are not supported for create provisioning operations.

3. To enable update of the attribute during provisioning operations, create a process task as follows:

   See Also: *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for detailed information about these steps

   a. Expand **Process Management,** and double-click **Process Definition.**

   b. Search for and open the **OIMTopsProvisioningProcess** process definition.

   c. Click **Add.**

   d. On the General tab of the Creating New Task dialog box, enter a name and description for the task and then select the following:

      Conditional

      Required for Completion

      Disable Manual Insert

      Allow Cancellation while Pending

      Allow Multiple Instances

   e. Click **Save.**

   f. Go to the Integration tab and click **Add.**

   g. In the Handler Selection dialog box, select **Adapter**, click **adpMODIFYTOPSUSER**, and then click the Save icon.

      The list of adapter variables is displayed on the Integration tab.

   h. To create the mapping for the first adapter variable:

      Double-click the number of the first row.

      In the Edit Data Mapping for Variable dialog box, enter the following values:

      Variable Name: `Adapter return value`

      Data Type: `Object`

      Map To: `Response code`

      Click the Save icon.

   i. To create mappings for the remaining adapter variables, use the data given in the following table:

Table 5–1 Values for the Variables, Map To, Qualifier, and Literal Value lists for each variable

Variable Number	Variable Name	Map To	Qualifier
Second	idfResource	Process Data	LDAP_SERVER
Third	uid	Process Data	LoginId

Table 5–1 (Cont.) Values for the Variables, Map To, Qualifier, and Literal Value lists for each variable

Variable Number	Variable Name	Map To	Qualifier
Fourth	attrName	String Literal	Enter the LDAP attribute name in the Literal Value field. Example: description Table 1–5, " Unmapped User Attributes for Target Resource Reconciliation and Provisioning" for a list of unmapped user attributes and their LDAP Gateway attribute names.
Fifth	attrValue	Process Data	Select the process form field from the drop-down list. Example: DESCRIPTION

j. On the Responses task, click **Add** to add at least the SUCCESS response code, with status C. This ensures that if the custom task is successfully run, then the status of task is displayed as Completed in Oracle Identity Manager.

k. Click the Save icon in the Editing Task dialog box, and then close the dialog box.

l. Click the Save icon to save changes to the process definition.

4. If you are using Oracle Identity Manager release 11.1.2 or later, create a new UI form and attach it to the application instance to make this new attribute visible. See Section 2.4.1.2, "Creating a New UI Form" and Section Section 2.4.1.6, "Updating an Existing Application Instance with a New Form" for the procedures.

5.4 Removing Attributes Mapped for Target Resource Reconciliation

The SingleValueAttributes and MultiValuedAttributes properties contain the list of target system attributes that are mapped for scheduled task reconciliation. These properties are found in the Top Secret Reconcile All Users and Top Secret Reconcile All LDAP Users scheduled tasks. If you want to remove an attribute mapped for scheduled task reconciliation, then remove it from the SingleValueAttributes or MultiValuedAttributes property.

5.5 Configuring the Connector for Provisioning to 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 all installations of the target system.

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

   See IT Resource in *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about creating IT resources.

   See Table 2–2, " IT Resource Parameters" 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 on the Oracle Identity Manager computer.

   > **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>
   ```

   When you change the port number, you must make the same change in the value of the idfServerPort parameter of the IT resource that you create by performing Step 1.

5. Save and close the beans.xml file.

6. Open the *LDAP_INSTALL_DIR*/conf/tops.properties file and set values for the following parameters:

   - _host_= Enter the IP address or host name of the mainframe.
   - _port_= Enter the port number for the second instance of the Provisioning agent.
   - _agentPort_= Enter the port number for 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. Save and close the tops.properties file.

8. In a Linux or Solaris environment, if there are not enough socket file descriptors to open up all the ports needed for the server, then:

   a. In a text editor, open the run script from the *LDAP_INSTALL_DIR*/bin directory.

b. Add the following line in the file:

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

c. Save and close the file.

When you perform provisioning operations:

When you use the Oracle Identity System Administration to perform provisioning, you can specify the IT resource corresponding to the CA Top Secret installation to which you want to provision the user.

5.6 Configuring the Generation of Single-Use Passwords for the Reset Password Operation

You can create and configure an adapter that generates single-use passwords when the Reset Password operation is performed. To create the adapter:

> **See Also:** *Oracle Fusion Middleware Performing Self Service Tasks with Oracle Identity Manager* for detailed information about the steps of this procedure

1. Use the Adapter Factory to create a copy of the ResetPassword adapter.
2. Add the following variables to the adapter that you create:

   passwordExpire: boolean or String

   passwordExpireInterval: String
3. The idm.jar file is located in the JavaTasks directory. When you create and map the new adapter task, use the following functions defined in this file:
   - public String resetPassword(String idfUserId, String idfNewPwd, boolean expire, String expireInDays)
   - public String resetPassword(String idfUserId, String idfNewPwd, String expireNow, String expireInDays)

   In these functions, the expire and expireNow parameters expect the value `true` to expire users' passwords.
4. Compile the adapter.
5. Create a process task, and associate it with the object corresponding to the event for which you want single-use passwords to be generated. For example, you can associate the process task with the Password Updated task or with the event that the PWD_EXP check box on the process form is selected.

5.7 Initial LDAP Gateway Population and Full Reconciliation

Instead of reconciling directly from the target system to OIM (which can be slow on large systems), the LDAP gateway offers an internal LDAP store that can be populated with target system users by using a single transaction to the mainframe. Oracle Identity Manager then reconciles user data from the LDAP store instead of the target system. Reconciling user, profile, and facility data from an extract file requires the following procedure:

5.7.1 Reconciliation Using a CFILE Extract File

This feature will perform full reconciliation 30% - 50% faster than the normal OOTB Scheduled Task that reconciles all users. This requires coordination with configuration changes for the Pioneer Mainframe Agent.

1. Have the Mainframe Team configure the Pioneer agent to use a generated file. (See Chapter 3, "Connector Deployment on the Mainframe"). Run the IRRXUTIL to use the EXTRACT USER or GROUP command that will generate the file of all users and data.
2. After file has completed above, open the *LDAP_INSTALL_DIR*/conf/tops.properties file.
3. Set the value for the _internalEnt_ property to true.
4. Save and close the property file.
5. Log into the Oracle Identity System Administration.
6. Search for and open the **Top Secret Reconcile Users to Internal LDAP** scheduled task.
7. Enter values for the scheduled task properties.

   Table 4–5 describes the attributes of the scheduled task.
8. Run the scheduled task. This task will initially populate the internal LDAP store with all user profiles.
9. Once the task has completed, search for and open the **Top Secret Reconcile LDAP Users to OIM** scheduled task.
10. Enter values for the scheduled task properties.

    Table 5–2 describes the attributes of the scheduled task.

Table 5–2 Attributes of the Reconcile LDAP Users to OIM Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: `TopSecretResource`
Resource Object	Enter the name of the resource object against which the reconciliation run will be performed. Sample value: `OIMTopSecretResourceObject`
Domain OU	Enter the name of the internally-configured directory in the LDAP store where the target system users will be retrieved. Sample value: `tops`
MultiValuedAttributes	Enter a comma-separated list of multivalued attributes that you want to reconcile. Do not include a space after each comma. Sample value: `profiles,facilities,groupIds`

Table 5–2 (Cont.) Attributes of the Reconcile LDAP Users to OIM Scheduled Task

Attribute	Description
SingleValueAttributes	Enter a comma-separated list of single-valued attributes that you want to reconcile. Do not include a space after each comma. Do not include attributes already listed in the MultiValueAttributes field. Sample value: `uid,owner,defaultGroup,waddr1,tsoMaxSize` **Note:** By default, Oracle Identity Manager's design form only allows entering up to 150 characters in a text field. To increase this limit, change the value of the TSA_VALUE column in the Oracle Identity Manager database.
LDAP Time Zone	Enter the time zone ID for the server on which the LDAP gateway is hosted. Sample value: `EST`
UID Case	Enter whether the user ID should be displayed in uppercase or lowercase. Sample value: `upper`
R2	Enter whether the release of Oracle Identity Manager being used is 11.1.2.*x*. Sample value: `true`

11. Run the scheduled task. This task will reconcile each user from the internal LDAP store to Oracle Identity Manager.

5.8 Configuring Windows Service

In a Windows environment, the LDAP gateway server can also be installed as a Windows Service. This section describes the installation and configuration procedure of the Windows Service for the LDAP Gateway.

Overview of the Installation Process

The Windows Service for the LDAP Gateway is installed using a supplied IdentityForge batch file. The batch file for the Windows service installer should be updated with your system's JAVA_HOME, JVM, HOME, and APPLICATION_SERVICE_HOME variables. The Windows service installer uses the Apache Procrun utility prunsrv.exe to create a fully managed Windows Service for the LDAP Gateway.

Installation Steps

To install and configure the Windows Service for the LDAP Gateway, you must perform the following steps:

1. In a text editor, open the **IDF-Win-Service.bat** file in the *<LDAP_INSTALL_DIR>/win_service* directory.

   Modify the *JAVA_HOME*, *JVM, HOME,* and *APPLICATION_SERVICE_HOME* variables to match your environment settings. In the following example, the *JAVA_HOME*, *JVM, HOME,* and *APPLICATION_SERVICE_HOME* environment variables are set:

   ```
   set JAVA_HOME=C:\software\Java\jdk1.7.0_55
   ```

```
set JVM=C:\software\Java\jdk1.7.0_55\jre\bin\server\jvm.dll
set HOME=D:\software\ldapgateway5.0
set APPLICATION_SERVICE_HOME=D:\software\ldapgateway5.0\win_service
```

2. To modify the default LDAP Gateway service name (LDAPGatewayService), perform the following steps:

   a. In IDF-Win-Service.bat file, update the "SERVICE_NAME" variable with the chosen custom service name: `set SERVICE_NAME=LDAPGatewayService432`

   b. In the /win_service directory, rename the LDAPGatewayService application to match the chosen custom service name.

3. To customize the log file locations, you must edit the CG_IDFLOG and CG_XMLERRLOG variables as follows:

   a. Locate the following section of the IDF-Win-Service.bat file:

   ```
   rem set CG_IDFLOG="-Didf.logpath="%CG_LOGPATH%\idfserver_custom.log"

   rem set
   CG_XMLERRLOG="-Didf.xmllogpath="%CG_LOGPATH%\idf.xml.error_custom.log"
   ```

   b. Uncomment the CG_IDFLOG and CG_XMLERRLOG variables and modify the variable paths to match your custom locations.

   c. Locate and uncomment the following lines in the IDF-Win-Service.bat file:

   ```
   rem set EXECUTE_STRING= "%EXECUTABLE%" //US//%SERVICE_NAME% ++JvmOptions
   %CG_IDFLOG%
   rem call:executeAndPrint %EXECUTE_STRING%
   rem echo .........

   rem set EXECUTE_STRING= "%EXECUTABLE%" //US//%SERVICE_NAME% ++JvmOptions
   %CG_XMLERRLOG%

   rem call:executeAndPrint %EXECUTE_STRING%

   rem echo .........
   ```

   d. Save and close the file.

4. Execute the following command from the command console from within the *<LDAP_INSTALL_DIR>/win_service* directory to install the service:

   ```
   > IDF_Win_Service install
   ```

5. If there are any problems with the installation of the service from the batch file, check the JAVA_HOME and JVM variables to make sure they are accurate.

6. Once the service is installed, you can start, stop, and restart it from the standard Windows Services manager.

Modifying or Removing the Windows Service

If you need to modify the windows service settings, it is recommended to first uninstall the service, make the modifications, and then re-install the service.

To uninstall the service, execute the following command from the *<LDAP_INSTALL_DIR>/win_service* directory:

```
> IDF_Win_Service remove
```

5.9 Customizing Log File Locations

The name and log location of the main LDAP gateway log file (idfserver.log) and the CFILE XML error log file (idf.xml.error.log) can be modified by adding additional arguments to the LDAP gateway server STARTUP command. These arguments are optional, and you can include one, both, or neither in the STARTUP command:

1. In a text editor, open the run script from the LDAP_INSTALL_DIR/bin directory. This run script is used to start and stop the LDAP gateway.

   (i) If using a Windows system, open the run.bat file.

   (ii) If using a UNIX system, open the run.sh file.

2. Add the arguments to the start command, located at the end of the run script:

   (i) The arguments should be added after the "-cp %CLASSPATH%" argument.

   (ii) To modify the idfserver.log path, use the argument -Didf.logpath=

   (iii) To modify the idf.xml.error.log path, use the argument -Didf.xmllogpath=

   In the following example, the start command will set the idfserver.log path to

   C:/logs/ldap/idfserver.log and the idf.xml.error.log path to C:/logs/errors/idf.xml.error.log:

   ```
   %JAVACMD% %DEBUG% %JVM_OPTS% %SECURE% -cp %CLASSPATH%
   -Didf.logpath="c:/logs/ldap/idfserver.log"
   -Didf.xmllogpath="c:/logs/errors/idf.xml.error.log"
   -Djava.library.path=%HOME%/lib com.identityforge.idfserver.Main %1 %2 %3 %4 %5
   %6 %7 %8 %9
   ```

6

Troubleshooting

Table 6–1 describes solutions to problems that you might encounter while using the connector.

Table 6–1 Troubleshooting Tips

Problem Description	Solution
The LDAP Gateway does not send the full attribute value when provisioning attribute values that contain one or more space characters.	If this problem occurs, surround the attribute value in single quotation marks when populating the form field.
IOException: The process cannot access the file because another process has locked a portion of the file. This error is thrown during LDAP Gateway server startup.	Ensure that there are no other LDAP Gateways running on the server. Often, this error occurs when an LDAP Gateway Windows service is started in the background and a user attempts to start another LDAP Gateway using the run.bat file.
Oracle Identity Manager cannot establish a connection with CA Top Secret.	■ Ensure that the mainframe server is up and running. ■ Verify that the required ports are working. ■ Due to the nature of the Provisioning Agent, 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. ■ Read the LDAP Gateway logs to determine if messages are being sent or received. ■ Verify that the IP address, administrator ID, and administrator password are correctly specified in the IT resource. See *Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for information about viewing and modifying IT resources. ■ Verify that the mainframe user account and password have not been changed.
The mainframe does not appear to respond.	Check the logs. If any of the mainframe JCL jobs have reached an abnormal end, then make the required corrections and rerun the jobs.

Table 6–1 (Cont.) Troubleshooting Tips

Problem Description	Solution
A particular use case does not appear to be functioning.	Check for the use case event in the LDAP Gateway logs. Then check for the event in the specific log assigned to the CA Top Secret Advanced connector that you are using. ■ If the event does not register in either of these two logs, then investigate the connection between Oracle Identity Manager and the LDAP Gateway. ■ If the event is in the log but the command has not had the intended change on a mainframe user, then check for configuration and connections between the LDAP Gateway and the mainframe. ■ Verify that the message transport layer is working.
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 event data is sent to the subpool cache. If the mainframe fails, then all messages are written to the disk. When this happens, restart the Reconciliation Agent so that it reads messages from the disk or subpool cache and resends the messages.
The LDAP Gateway does not respond to reconciliation requests when installed as a Windows service.	Check that the /lib directory in the LDAP Gateway does not contain multiple versions of the same JAR file. The Windows Service script installs all files in the /lib directory. Therefore, having multiple versions of the same JAR file can result in a collision. See the run script located in the /bin directory for the correct name and version number of the JAR file.

7 Known Issues and Workarounds

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

- **Bug 21308336**

  The reconciliation scheduled tasks have parameters for trusted reconciliation settings even though the connector no longer supports trusted reconciliation.

- **Bug 21116938**

  No CFILE reconciliation support for WA attributes.

- **Bug 21070686**

  When configuring custom log file locations, any custom directories must already exist on the file system, otherwise the log file will not be generated.

- **Bug 21137273**

  When configuring a provisioning update process task for CICS SITRAN or CICS SITRAN FACILITY fields, the process task must be mapped to the adpModifySitranTopsUser adapter (instead of the standard adpModifyTopsUser adapter), or the provisioning update will fail due to a malformed TSS command.

- **Bug 18781115**

  When there is a mismatch between the encryption key used by the LDAP and mainframe agents, neither the LDAP gateway nor the agent specifies the mismatch in the log file.

- **Bug 18781177**

  The Voyager agent cannot parse spaces or null values in the control file MSGID01 parameter. If there are spaces or null entries in the parameter, Voyager will ABEND.

- **Bug 18781303**

  When running reconciliation using a secondary IT resource, the "Last Modified Time Stamp" parameter of the secondary IT resource is not updated when the task completes.

- **Bug 19491412**

  Voyager reconciled Oefilep as Oeflep.

- **Bug 19491399**

  CFILE reconciles Oecputm as olecputm.

- **Bug 19491200**

  CFILE and TSS to OIM scheduled task parse cicsSctykey as cicsSctkey.

- **Bug 19491188**

  Provisioning operation on the following attributes are not working: misc1, misc2, misc3, misc4, misc5, misc6, misc7, misc8, misc9, tsoAcct, tsoAuth, tsoPrfg, and tsoProc.

- **Bug 19828702**

  The LDAP Gateway does not send the full attribute value when provisioning attribute values that contain one or more space characters.

A

Authorized Libraries

APF means "Authorized Program Facility". In a z/OS environment, APF is a facility that permits the identification of programs that are authorized to use restricted functions. APF-authorized programs must reside in one of the following authorized libraries:

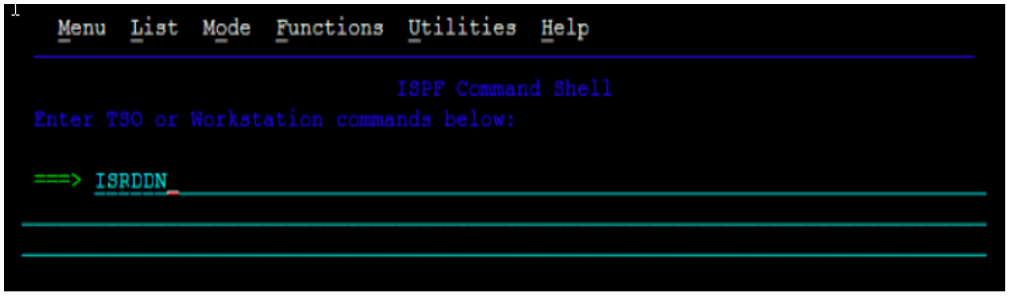
- SYS1.LINKLIB
- SYS1.SVCLIB
- SYS1.LPALIB
- Authorized libraries specified by your installation

Authorized libraries are defined in an APF list. APF also prevents authorized programs (supervisor state, APF-authorized, PSW key 0-7, or PKM 0-7) from accessing a load module that is not in an APF-authorized library.

To find the datasets those are APF authorized:

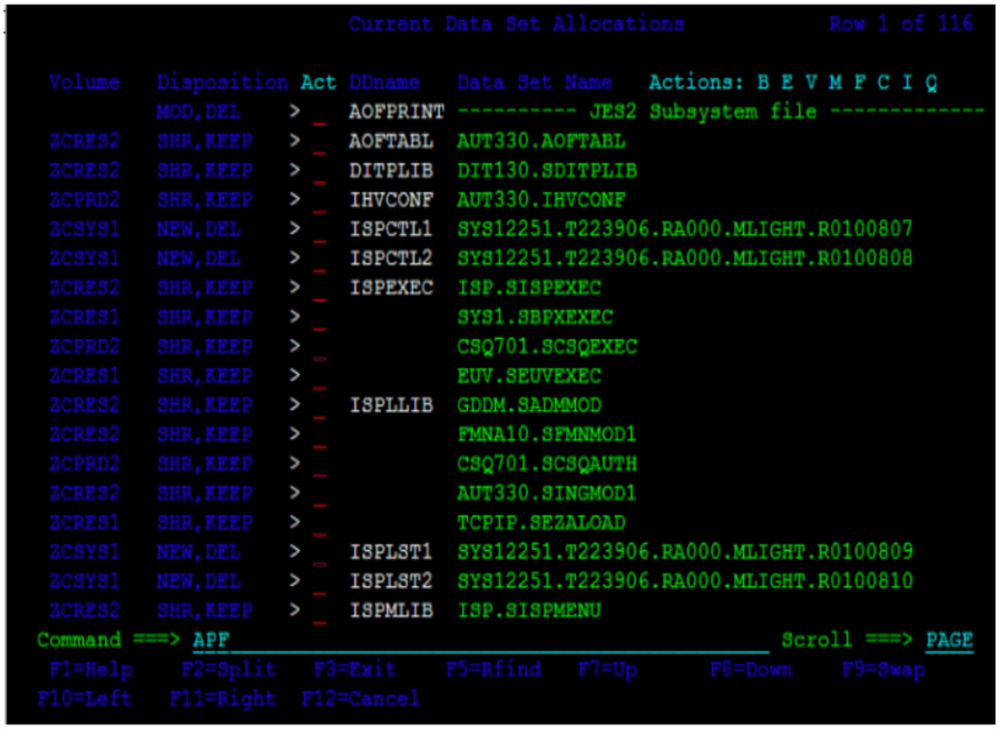
1. Type TSO ISRDDN in your ISPF session (some shops need just ISRDDN with no TSO prefix) and press **enter**.
2. Type APF and press **enter**. It will bring up a list of all datasets that are APF authorized.

Remember that, if you like to use an APF authorized dataset in a job STEPLIB, make sure all the datasets in the STEPLIB are APF authorized.



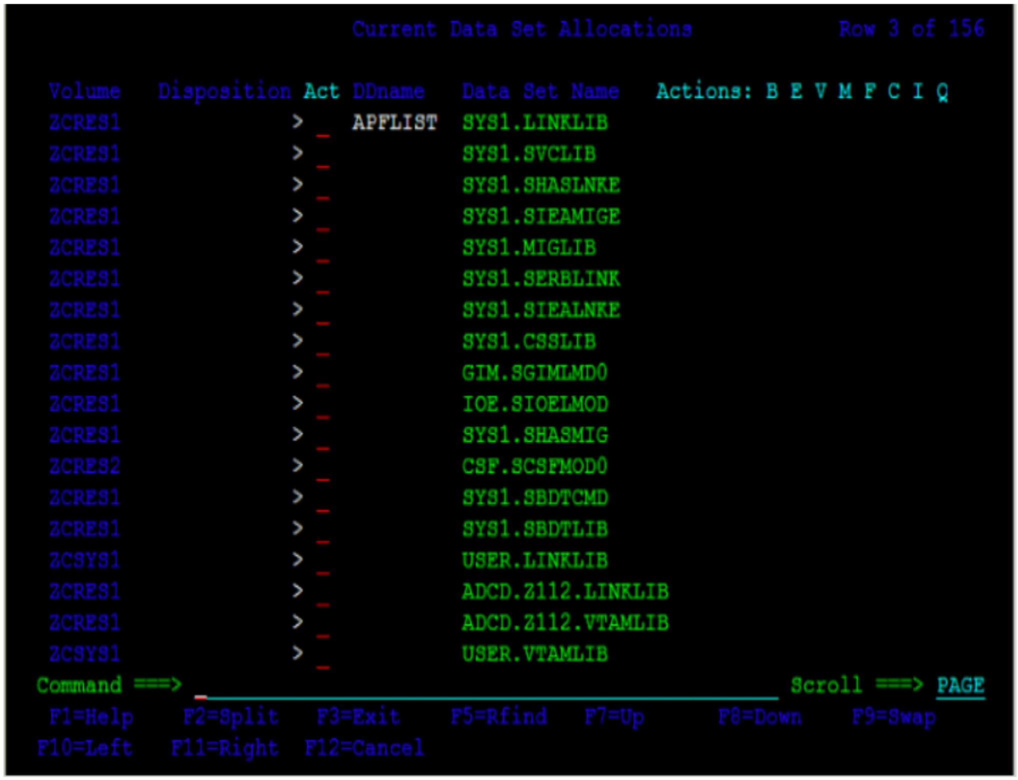
```
                    ISPF Command Shell
Enter TSO or Workstation commands below:

===> ISRDDN
```



```
                              Current Data Set Allocations            Row 1 of 116

  Volume   Disposition Act DDname   Data Set Name   Actions: B E V M F C I Q
           MOD,DEL      > _ AOFPRINT ---------- JES2 Subsystem file -------------
  ZCRES2   SHR,KEEP     > _ AOFTABL  AUT330.AOFTABL
  ZCRES2   SHR,KEEP     > _ DITPLIB  DIT130.SDITPLIB
  ZCPRD2   SHR,KEEP     > _ IHVCONF  AUT330.IHVCONF
  ZCSYS1   NEW,DEL      > _ ISPCTL1  SYS12251.T223906.RA000.MLIGHT.R0100807
  ZCSYS1   NEW,DEL      > _ ISPCTL2  SYS12251.T223906.RA000.MLIGHT.R0100808
  ZCRES2   SHR,KEEP     > _ ISPEXEC  ISP.SISPEXEC
  ZCRES1   SHR,KEEP     > _          SYS1.SBPXEXEC
  ZCPRD2   SHR,KEEP     > _          CSQ701.SCSQEXEC
  ZCRES1   SHR,KEEP     > _          EUV.SEUVEXEC
  ZCRES2   SHR,KEEP     > _ ISPLLIB  GDDM.SADMMOD
  ZCRES2   SHR,KEEP     > _          FMNA10.SFMNMOD1
  ZCPRD2   SHR,KEEP     > _          CSQ701.SCSQAUTH
  ZCRES2   SHR,KEEP     > _          AUT330.SINGMOD1
  ZCRES1   SHR,KEEP     > _          TCPIP.SEZALOAD
  ZCSYS1   NEW,DEL      > _ ISPLST1  SYS12251.T223906.RA000.MLIGHT.R0100809
  ZCSYS1   NEW,DEL      > _ ISPLST2  SYS12251.T223906.RA000.MLIGHT.R0100810
  ZCRES2   SHR,KEEP     > _ ISPMLIB  ISP.SISPMENU
 Command ===> APF                                             Scroll ===> PAGE
  F1=Help     F2=Split    F3=Exit     F5=Rfind    F7=Up       F8=Down     F9=Swap
 F10=Left    F11=Right   F12=Cancel
```



```
                              Current Data Set Allocations            Row 3 of 156

  Volume   Disposition Act DDname   Data Set Name   Actions: B E V M F C I Q
  ZCRES1                > _ APFLIST  SYS1.LINKLIB
  ZCRES1                > _          SYS1.SVCLIB
  ZCRES1                > _          SYS1.SHASLNKE
  ZCRES1                > _          SYS1.SIEAMIGE
  ZCRES1                > _          SYS1.MIGLIB
  ZCRES1                > _          SYS1.SERBLINK
  ZCRES1                > _          SYS1.SIEALNKE
  ZCRES1                > _          SYS1.CSSLIB
  ZCRES1                > _          GIM.SGIMLMD0
  ZCRES1                > _          IOE.SIOELMOD
  ZCRES1                > _          SYS1.SHASMIG
  ZCRES2                > _          CSF.SCSFMOD0
  ZCRES1                > _          SYS1.SBDTCMD
  ZCRES1                > _          SYS1.SBDTLIB
  ZCSYS1                > _          USER.LINKLIB
  ZCRES1                > _          ADCD.Z112.LINKLIB
  ZCRES1                > _          ADCD.Z112.VTAMLIB
  ZCSYS1                > _          USER.VTAMLIB
 Command ===> _                                               Scroll ===> PAGE
  F1=Help     F2=Split    F3=Exit     F5=Rfind    F7=Up       F8=Down     F9=Swap
 F10=Left    F11=Right   F12=Cancel
```

B

AES 128 User Key Definition and Usage

Pioneer and Voyager agents support the use of AES128 user key definitions. The customized key should consist of ASCII characters. Specifically, ASCII codes 33 – 127 are supported.

To change the pre-configured key, perform the following steps:

1. Copy the KEYMODR JCL to a new member in the PDS.
2. The Job stream is an AMASZAP, the module name is IDFRINFO.
3. Verify that the //SYSLIB is pointing to the LOADLIB or LINKLIB where Pioneer/Voyager modules are located.
4. Edit the copied member and modify the "REP 008A", the key is 32 bytes long.
5. Do not change REP displacement REP 009A and 00AA
6. Change REP 00BA to the date of the above change.
7. Submit the Job stream.

> **Note:** The AES128 key change effects both Pioneer/Voyager. Once an AES128 key is changed as stated above, shutdown Pioneer/Voyager and restart. Also the properties file on the LDAP must also be changed to contain the same key.

The LDAP gateway server settings must also be updated to use the new key. To configure the LDAP gateway, perform the following steps:

1. Stop the LDAP gateway server (if it is running).
2. Open the tops.properties file, located in the *LDAP_INSTALL_DIR*/conf directory.
3. Modify the value of the _secretKey_ property to match the new key.
4. Save and close the file.
5. Restart the LDAP gateway server.

C

Top Secret CFILE -> LDAP Attribute Mapping

Note: Only a user's profiles and facilities child data is reconciled through CFILE reconciliation. No other child values are reconciled.

Table C–1 lists CFILE record#, record type, LDAP attribute and the corresponding descriptions.

Table C–1 CFILE LDAP Attribute Mapping

CFILE RECORD #	RECORD TYPE	LDAP ATTRIBUTE	DESCRIPTION
	ACCESSORID	uid	ACID Unique ID
0100	NAME	cn	Full Name
0200	TYPE	type	ACID Type (USER, PROFILE, etc)
0300	DEPT ACID	deptAcid	Department ID
0300	DEPT NAME	department	Department Descriptive Name
0400	DIV ACID	divAcid	Division ID
0400	DIV NAME	division	Division Descriptive Name
0450	ZONE ACID	zoneAcid	Zone ID
0450	ZONE NAME	zone	Zone Description Name
0500	CREATED	createDate	Create Date
0500	LAST MOD	lastModificationDate	Modify Date
0501	EXPIRES	expires	Expire Date
0502	SUSPENDED	suspendedUntilDate	Suspend Date
0600	PROFILES	profiles, memberOf	Profile Acids, Profile Acids Dn
0650	GROUPS	groupIds, groupOf	Group Acids, Group Acids Dn
0700	ATTRIBUTES	attributes	Security Attributes
0800	BY PASSING	bypassing	Security ByPassing Attributes
0900	LAST USED	lastUsed	Last Used Date
1000	MASTER FAC	xresource	
1100	LOCK TIME	lockTime	
1200	LANGAUGE	language	Language
2002	XA DATASET	xresources	SEE BELOW (#A)

Table C–1 (Cont.) CFILE LDAP Attribute Mapping

CFILE RECORD #	RECORD TYPE	LDAP ATTRIBUTE	DESCRIPTION
2005	XA xxxx (RESOURCE)	xresources	SEE BELOW (#B)
2014	PRIVPGM	xresources	SEE BELOW
2021	ACCESS	xresources	
2016	ACTION	xresources	
2100	FACILITY	facilities, facilityOf	Facility Acid, Facility Acid Dn
2200	SOURCES	sources	Source ACID
2300	OPIDENT	cicsOpident	CICS Operator Identification Value
2300	OPPRTY	cicsOpprty	CICS Operator Priority
2301	SITRAN	cicsSitran, cicsSitranFacility	CICS Transaction Following Facility Sign-In, CICS Facility Associated With Transaction
2400	OPCLASS	cicsOpclass	CICS Operator Classes
2500	SCTYKEY	cicsSctykey	CICS Security Keys
2600	INSTDATA	Instdata	255 Byte Text Field
2700	USER		
2800	ACID	uniqueIds uniqueMember	Acids Profile Mem, Acids Dn
2901	FACILITIES	facilitiesp	Admin Facilities
2902	ACID	acid	Admin Acid
2903	LIST DATA	listData	Admin List Data
2904	MISC1	misc1	Admin Authority
2905	MISC9	misc9	Admin Authority
2906	RESOURCES	res	Admin Authority
2907			
2908	MISC2	misc2	Admin Authority
2909	SCOPE	scope	Admin Authority
2910	MISC8	misc8	Admin Authority
2911	ACCESS	access	Admin Authority
2912	MISC3	misc3	Admin Authority
2913	MISC4	misc4	Admin Authority
2914	MISC5	misc5	Admin Authority
2921	ACCESS	xresources	See Below
3000	PASSWORD	passwordExpireDate passwordExpireInterval	Password Info
3500	TSOLPROC	tsolproc	TSO Logon Proc
3501	TSOLACCT	tsolacct	TSO Logon Account
3502	TSOJCLASS	tsojclass	TSO Job Class
3503	TSOMCLASS	tsomclass	TSO Message Class
3504	TSOLSIZE	tsolsize	TSO Region Size

Table C–1 (Cont.) CFILE LDAP Attribute Mapping

CFILE RECORD #	RECORD TYPE	LDAP ATTRIBUTE	DESCRIPTION
3505	TSOUDATA	tsoudata	TSO User Data
3506	TSODEFPRFG	tsodefprfg	TSO Performance Group
3507	TSOOPT	tsoopt	TSO Options
3508	TSOCOMMAND	tsocommand	TSO Logon Command
3509	TSODEST	tsodest	TSO Output Destination
3510	TSOHCLASS	tsohclass	TSO Hold Class
3511	TSOMSIZE	tsomsize	TSO Max Region Size
3512	TSOSCLASS	tsosclass	TSO Sysout Class
3513	TSOUNIT	tsounit	TSO Unit
3700	FACILITY	facilities	Facility, All
4011 and 4012	USER-DEFINED	User Defined	User Defined Field Attribute will Match Field Name
4011	#APPL	lu62#appl	LU 6.2 #Appl
4011	#ENTITY	lu62#entity	LU 6.2 #Entity
4011	BC1CHAIN	lu62bc1chain	LU 6.2 Bc1chain
4011	BC2CHAIN	lu62bc2chain	LU 6.2 Bc2chain
4011	SET1DISP	lu62set1disp	LU 6.2 Set1disp
4011	SET2DISP	lu62set2disp	LU 6.2 Set2disp
4011	NETVCONS	netviewConsname	Netview Console Identifier
4011	NETVCTL	netviewControl	Netview Security Check Type
4011	NETVDMNS	netviewDomains	Netview Cross-Domain Sessions
4011	NETVIC	netviewInitCms	Netview Initial Command
4011	NETVMSGR	netviewMsgrecvr	Netview Receive Unsolicited Messages
4011	NETVNGMF	netviewNgmfadmn	Netview Authority To Graphic Monitor Facility
4011	NETVOPCL	netviewOpclass	Netview Scope Classes
4401	UID	omvsUid	Omvs User ID
4402	GID	omvsGid	Omvs Group ID
4403	HOME	omvsHome	Omvs Home Subdirectory
4404	OMVSPRGM	omvsProgram	Omvs Program
4405	DFLTGRP	defaultGroup	Omvs Default Group
4406	ASSIZE	omvsAssize	Omvs Max Address Space Size
4407	MMAPAREA	omvsMmapArea	Omvs Max Data Space Pages
4408	OECPUTM	olecputm	Omvs Max Cpu Time
4409	OEFILEP	omvsOefilep	Omvs Max Files Per Process
4410	PROCUSER	omvsprocuser, procuser	Omvs Max Processes
4411	THREADS	omvsThreads	Omvs Max Pthreads Created

LDAP ATTRIBUTE -> XRESOURCES

User is expected to read the xresources attribute and parse the data as needed for their application use.

:: Separates Field Name::Field Value

| Separates Different Fields

EXAMPLE DATA FOR DIFFERENT TYPES ->

acid-res::ACID|acid-auth::AMPIO#T|

rclass::$MOBIUS|rowner::DSAPP1|rres::DS.|alevel::READ|authfac::MOBIUST|authfac::MOBIUSP|

xauthclsn::DATASET|xauthdsno::DATASEX|xauthdsn::TXXXA.DUMMY4|alevel::READ|authfac::CICSPROD|authfacs::CICSTEST|

D

Top-Secret CFILE Processing

This appendix describes Top-Secret CFILE processing.

This release supports a new function. The function is a full Recon. The input for the Recon is the Top-Secret CFILE.

Below is typical JCL used to create the CFILE.

```
//TSSCFILE JOB ,SYSTEMS,CLASS=A,MSGCLASS=X,
//      MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID
//STEP1   EXEC  PGM=TSSCFILE,PARM='PRINTDATA',REGION=0M
//PRINT   DD    SYSOUT=*
//OUT     DD    DSN=yourhlq.CFILE.FILE,DISP=SHR
//IN      DD    *
  TSS LIST(ACIDS) TYPE(USER) DATA(PROF,PASS,ALL)
/*
```

After creating a CFILE the following job reformats the data from 300 bytes to 320 bytes.

*** Fixed record file format – RECFM=FB ***

```
//CFILECPY JOB ,SYSTEMS,CLASS=A,MSGCLASS=X,
//      MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID
//STEP1   EXEC  PGM=CFILECPY
//CFILEIF  DD   DSN=yourhlq.CFILE.FILE,DISP=SHR
//CFILEOUT DD   DSN=yourhlq.CFILE.OUT,DISP=SHR
/*

***  Variable record file format - RECFM=VB ***
//CFILECPY JOB ,SYSTEMS,CLASS=A,MSGCLASS=X,
//      MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID
//STEP1   EXEC  PGM=CFILECPY
//CFILEIV  DD   DSN=yourhlq.CFILE.FILE,DISP=SHR,
//                DCB=(RECFM=VB,LRECL=304)
//CFILEOUT DD   DSN=yourhlq.CFILE.OUT,DISP=SHR
/*
```

Then the last job converts the reformatted data into XML format.

```
//CFILECPY JOB ,SYSTEMS,CLASS=A,MSGCLASS=X,
//      MSGLEVEL=(1,1),REGION=0M,NOTIFY=&SYSUID
//STEP1   EXEC  PGM=CONV2XML
//LINEOUT  DD   SYSOUT=*
//SYSPRINT DD   SYSOUT=*
//CFILEIN  DD   DSN=yourhlq.CFILE.OUT,DISP=SHR
//CFILEXOT DD   DSN=yourhlq.CFILE.XML,DISP=SHR
/*
```

The CFILEXOT ddname is the same filename as the Pioneer EXPORTIN ddname. They must match. After the file is created the LDAP will request the file and pick it up. Upon successful reading of the file and transporting of the data to the LDAP the file is closed and cleared. The following are the only CFILE record types that these utilities will process, any other record types will be rejected.

```
* 100,200,300,400,500,501,502,600,650,  *
* 700,800,900,1200,2100,2200,2300,2400, *
* 2500,2600,2700,2901,2902,2903,2904,   *
* 2905,2906,2907,2908,2909,2910,2911,   *
* 2912,2913,2914,3000,3500,3501,3502,   *
* 3503,3504,3505,3506,3507,3508,3509,   *
* 3510,3511,3512,3513,4010,4011,4012,   *
* 4401,4402,4403,4404,4405,4406,4407,   *
* 4408,4409,4410,4411,2002,2005,2021,   *
* 2301,3700                             *
```

E

Provisioning Methods for OIM Adapters

The connector supports additional provisioning operations to CA Top Secret that are not shipped with a pre-configured child form, process task, or OIM adapter. Below is a list of method headers for functions included in the com.identityforge.idfTopsUserOperations java class (located in the topsecret-provisioning-adapter.jar). You can access these methods when creating or modifying an OIM adapter:

Primary Constructor:

```
public IdfTopsUserOperations(String idfServerHost, String idfServerPort, String
idfRootContext, String idfPrincipalDn, String idfPrincipalPwd, String ssl, String
trustStore, String trustStorePassword, String trustStoreType) throws Exception
```

Method Headers:

```
public String changePassword(String idfUserId, String idfCurrentPwd, String
idfNewPwd)
public String deleteUser(String idfUserId)
public String resetPassword(String idfUserId, String idfNewPwd)
public String resetPassword(String idfUserId, String idfNewPwd, String expireNow,
String expireInDays)
public String revokeUser(String idfUserId)
public String revokeUser(String userId, String revokeUntil, String revokeFor)
public String revokeUserUntil(String userId, String revokeUntil)
public String resumeUser(String idfUserId)
public String resumeUserUntil(String userId, String type, String until)
public String resumeUser(String userId, String type, String until)
public String renameUser(String idfUserId, String newUid)
public String modifyUser(String idfUserDn, String idfAttrName, String
idfAttrValue)
public String modifyUserRemove(String idfUserDn, String idfAttrName, String
idfAttrValue)
public String grantTsoAccess(String idfUserId, String idfTsoCommand, String
idfTsoAcctNum, String idfTsoSize, String idfTsoMaxSize, String idfTsoDest, String
idfHoldClass, String idfMsgClass, String idfJobClass, String idfProc, String
idfSysOutClass, String idfUnit, String idfUserData, String idfOpt)

public String addUserToDataset(String idfUserId, String idfDatasetId, String
idfAccess)
public String addUserToDataset(String userId, String datasetId, String access,
String accessFor)
public String addUserToFacility(String idfUserId, String idfFacility, String
idfAccess)
public String addUserToGroup(String idfUserId, String idfGroupId)
public String addUserToGroup(String uid, String groupId, String after, String
before, String first, String last, String forTime)
public String addUserToProfile(String uid, String profileId, String after, String
before, String first, String last, String forTime)
public String addUserToSource(String idfUserId, String idfSourceId)
public String removeUserFromDataset(String idfUserId, String idfDatasetId)
public String removeUserFromFacility(String idfUserId, String idfFaciltiy)
public String removeUserFromGroup(String idfUserId, String idfGroupId)
public String removeUserFromProfile(String uid, String profileId)
public String removeUserFromSource(String idfUserId, String idfSourceId)
public String generateCertificate(String idfUserId, String digicert, String dcdsn,
String keysize, String keyusage, String nbdate, String nbtime, String nadate,
String natime, String lablcert, String altname, String subjectn, String signwith,
String icsf, String dsa, String pcicc)

public String generateCertificateRequest(String idfUserId, String digicert, String
dcdsn, String lablcert)
```

F

LOADDSN Member and the File Contents

The Table F–1 shows the relationship between the steps in the LOADDSN member and the file contents that are loaded into PIONEER's datasets. In these example datasets, PIONEER is used for the High-Level qualifier for PIONEER files and VOYAGER is used for the High-Level qualifier for VOYAGER files. The HLQ will have to be changed to meet installation standards.

Table F–1 Steps of LOADDSN Member and File Contents

Steps	File Contents

Step #1	//STEP1 EXEC PGM=IEBGENER
	//* SYSUT2 = PIONEER DDNAME - RECONJCL
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(REXXCL),DISP=SHR
	//SYSUT2 DD DSN=PIONEER.RECON.LIBRARY,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

REXXCL	//REXXCLST JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
	// NOTIFY=&SYSUID,REGION=0K
	//STEP0 EXEC PGM=IKJEFT01,DYNAMNBR=50
	//SYSTSPRT DD SYSOUT=*
	//SYSPRINT DD SYSOUT=*
	//FILEOUT DD DISP=SHR,DSN=PIONEER.RECON.FILE <--- Pioneer's //RECONOUT
	//SYSPROC DD DISP=SHR,DSN=IDF.PROD.CLISTLIB
	//SYSTERM DD DUMMY
	//SYSTSIN DD *
	/*

Table F–1 (Cont.) Steps of LOADDSN Member and File Contents

Steps	File Contents

Step #2	//STEP2 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(ALIASLST),DISP=SHR
	//SYSUT2 DD DSN=PIONEER.INJCL.LIBRARY,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

ALIASLST	//IDCALIAS JOB SYSTEMS,MSGLEVEL=(1,1),MSGCLASS=X,CLASS=A,PRTY=8,
	// NOTIFY=&SYSUID,REGION=0K
	//STEP0 EXEC PGM=IDCAMS
	//SYSPRINT DD DSN=PIONEER.ALIAS.LSTOUT,DISP=SHR <-- Pioneer's //LISTINR
	//SYSIN DD *
	&CONTROL
	/*

Step#3	//STEP3 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(PSAMPLE),DISP=SHR
	//SYSUT2 DD DSN=PIONEER.CONTROL.FILE,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

PSAMPLE	TCPN=TCPIP
	IPAD=0.0.0.0
	PORT=5799
	DEBUG=N
	ESIZE=16
	LPAR=YOUR-LPAR
	RWAIT=???
	JWAIT=???
	POST_PROC_ALIAS=F
	IDLEMSG=N
	DEBUGOUT=SYSOUT,CLASS(?)
	SPIN_CLASS=?
	QUEUE_DSN=?
	AUDIT_LOG=NO
	EXPORT_MON,REC=?????
	LONG_FDTNAMES=Y,DSN=<YOURHLQ.DATASETNAME>

Table F–1 (Cont.) Steps of LOADDSN Member and File Contents

Steps	File Contents

Step#4	//STEP4 EXEC PGM=IEBGENER
	//SYSUT1 DD DSN=IDF.PROD.JCLLIB(VSAMPLE),DISP=SHR
	//SYSUT2 DD DSN=VOYAGER.CONTROL.FILE,DISP=SHR
	//SYSPRINT DD SYSOUT=*
	//SYSIN DD DUMMY

VSAMPLE	* SAMPLE CONTROL FILE FOR USERS USING IP ADDRESSES TO
	* CONNECT TO THE LDAP GATEWAY
	SUBPOOL_SIZE=1000K
	TCPN=TCPIP
	IPAD=???.???.???.???
	PORT=?
	DEBUG=N
	ESIZE=16
	VOYAGER_ID=????????
	CACHE_DELAY=???
	AUDIT_LOG=NO
	PIONEER_DELETE_MSGS=NO
	CONNECT_MSGS=Y
	RECOVERY_INTERVAL=001,MINS
	LONG_FDTNAMES=Y,DSN=<YOURHLQ.DATASETNAME>

G

Reconciliation Agent (Voyager) Messages

This appendix describes log messages generated by the Reconciliation Agent.

> **Note:** All Reconciliation Agent messages are prefixed with `IDMV`.

Message:	**IDMV000I** Voyager Reconciliation Agent Starting
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV000I** Voyager is Executing from an APF Authorized Library
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV000E** Voyager is Not Executing from an APF Authorized Library
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV000I** Voyager Found TPSS Security Subsystem
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV000I** Voyager Found Required Storage Subpool
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV001I** Voyager Input Parameters are OK
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV002I** Voyager Build Level is at yyyymmddHHMM
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV004I** Voyager Detects (TCPIP) Jobname XXXXXXXX
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV005I** Voyager Detects (TCPIP) IP Address of
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV006I** Voyager Detects (TCPIP) IP PORT xxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV007I** Voyager Detects Encryption is ON
Message-Type:	Informational
Action Required:	None
Conditions:	When ESIZE is not 00 (Encryption ON)
Output:	Console, SYSOUT

Message:	**IDMV009I** Voyager Detects Cache File Opened OK
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV011I** Voyager Detects Encryption
Message-Type:	Informational
Action Required:	None
Conditions:	When ESIZE is 00 (Encryption ON)
Output:	Console, SYSOUT

Message:	**IDMV012I** Voyager Detects Debugging is ON
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug ON
Output:	Console, SYSOUT

Message:	**IDMV013I** Voyager Detects Debugging is OFF
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug Off
Output:	Console, SYSOUT

Message:	**IDMV014I** Voyager Detects MVS Retcodes of xxx
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV015I** Voyager Detects Country Code of XX
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV016E** Voyager Detects Bad Hostname of xxxxxxxxxx.xxx
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV016I** Voyager Detects Hostname of xxxxxxxxxx.xxx
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMV019E** Voyager Initialization of TCP API Failed RC: xx
Message-Type:	Error
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMV019I** Voyager Initialization of TCP API was Successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV020I** Voyager Initialization of GETCLIENTID was Successful
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV020E** Voyager TCPIP Socket Descriptors Exceeded - Fatal Error
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV021E** Voyager Initialization of PTON failed RC: xx
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV021I** Voyager Accepting Messages on xxx.xxx.xxx.xxx (OR) hostname.com
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV021I** Voyager Initialization of PTON was Successful
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMV025I** Voyager Connected to Gateway Server
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV025I** Connect messages will not be displayed
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	SYSOUT

Message:	**IDMV025I** Connect messages will be displayed
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	SYSOUT

Message:	**IDMV050I** Voyager Cache Polling Begins
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV051I** Voyager Cache Polling Ends
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV070I** Voyager <DD filename> is Now Open
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV071I** Voyager <DD filename> is Now Closed
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On, Unconditional
Output:	SYSOUT

Message:	**IDMV070E** Voyager could not open <DD File name> RC: <Return code>
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV001E** Voyager Input Control File is Empty
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV100I** Voyager Shutdown Started
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV101I** Voyager Found Storage Token
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV102E** Voyager Cache Dasd File Not be Found
Message-Type:	Error
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message: **IDMV102I** Voyager Storage Token Deleted RC = 0

Message-Type: Informational

Action Required: None

Conditions: Not Utilized

Output: Not Utilized

Message: **IDMV103I** Voyager has Ended with Non-Zero Return Code

Message-Type: Informational

Action Required: None

Conditions: Unconditional

Output: Console, SYSOUT

Message: **IDMV104I** Voyager Sent Messages nnnnn Received Messages nnnnn

Message-Type: Informational

Action Required: None

Conditions: Unconditional

Output: Console, SYSOUT

Message: **IDMV105I** Voyager Sent Bytes nnnnn Subpool Messages nnnnn

Message-Type: Informational

Action Required: None

Conditions: Unconditional

Output: Console, SYSOUT

Message: **IDMV110I** Voyager Reconciliation Agent has Terminated

Message-Type: Informational

Action Required: None

Conditions: Unconditional

Output: Console, SYSOUT

Message:	**IDMV111I** Voyager has Ended with Zero Return Codes
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV130I** Voyager Probed Server <n> Tries
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMV205E** Voyager Connection Retry Timer Exceeded
Message-Type:	Error
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV206E** Voyager Run Startup To Allocate Sp231
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV206E** Voyager Cachesav Open for Input Failed RC <Code> SEE SYSLOG
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV206E** Voyager Cachesav Close Failed RC: <Code> SEE SYSLOG
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV206I** Voyager Cachesav Open For Output
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV207I** Voyager CACHESAV Open for Input
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV208I** Voyager Reads nnnnn CACHE Messages
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV209I** Voyager Wrote nnnnn CACHE Messages
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV209I** Voyager Cacehsv Closed OK
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV210I** Voyager CACHESAV Cleared for Usage
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV151I** Voyager DNS Request Hostname.com
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMV151I** Voyager DNS Request Hostname.com
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV152I** Voyager IP Connect Request xxx.xxx.xxx.xxx
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMV200E** Voyager Config Parm Error - xxxxx
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV202E** Voyager no Storage Token Found
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV202I** Voyager Unable to Connect to new IP/Port
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV203E** Voyager Quiescing Because of the Subpool Not found
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV204E** Voyager Subpool 231 Cannot be Found
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV300I** *Debug* - xxxxxxxxxxxxxxxxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	DEBUGOUT

Message:	**IDMV401I** *DEFAULT* <PARM - TEXT>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional, If Debug On
Output:	Console, SYSOUT

Message:	**IDMV601I** Voyager Recovery Initiated
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMV601I** Voyager IP-FUNC (GETCLIENTID) ERRNO (n)
Message-Type:	Informational
Action Required:	None.
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV601I** Voyager IP-FUNC (SOCKET) ERRNO (n)
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV601I** Voyager IP-FUNC (PTON) ERRNO (n)
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV601I** Voyager IP-FUNC (SHUTDOWN) ERRNO (n)
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV601I** Voyager IP-FUNC (CLOSE) ERRNO (n)
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV602E** Voyager Connection Failed to LDAP - ERRNO(nnnnnn)
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMV603I** *CLISTI*
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV500I** *HEADER* - <Func> <CMD> <ACID> <STAT> <INFO>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	AUDITLOG

Message:	**IDMV500I** GENERIC <Func> <CMD> <ACID> <STAT> <INFO>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	AUDITLOG

Message:	**IDMV604I** Write Successful - MSG=(A=x,P=xxxx,L=nnnnnn, U=xxxxxxxx)
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMV999T** Write Good TRANS-CTR: nnnnn
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug is On
Output:	SYSOUT

Message:	**IDMV999E** Voyager is Abending due to Bad Parms
Message-Type:	Error
Action Required:	None
Conditions:	When Voyager Abends
Output:	Console

Message:	**IDMV999E** Please review Voyager SYSLOG
Message-Type:	Error
Action Required:	None
Conditions:	When Voyager Abends
Output:	Console

Message:	**IDMV999E** Voyager is Abending
Message-Type:	Error
Action Required:	None
Conditions:	When Voyager Abends
Output:	Console

Message:	**IDMV999E** Voyager has Abended
Message-Type:	Error
Action Required:	None
Conditions:	When Voyager Abends
Output:	Console

H

Provisioning Agent (Pioneer) Messages

This appendix describes messages generated by the Provisioning Agent.

Note: All Reconciliation Agent messages are prefixed with `IDMP`.

Message:	**IDMP000I** Pioneer Starting
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP001I** Pioneer Input Parameters are OK
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP001E** Pioneer Input Control File is Empty
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP002I** Pioneer Detects IDF-Build yyyymmddHHMM
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP003I** Pioneer Detects TCPIP Jobname XXXXXXXX
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP004I** Pioneer Detects TCPIP IP Address of xxx.xxx.xxx.xxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP005I** Pioneer Detects TCPIP IP PORT of xxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP006I** Pioneer Detects Debugging is ON/OFF
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMP007I** Pioneer Detects Audit log is <value>
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMP008I** Pioneer Detects KVER xxxxxxxxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP009I** Pioneer Detects Encryption Enabled
Message-Type:	Informational
Action Required:	None
Conditions:	If ESIZE=16 (Encryption ON)
Output:	Console, SYSOUT

Message:	**IDMP010I** Pioneer Detects Encryption Disabled
Message-Type:	Informational
Action Required:	None
Conditions:	If ESIZE NOT=16 (Encryption OFF)
Output:	Console, SYSOUT

Message:	**IDMP011I** Pioneer Detects CPUID xxxxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP012I** Pioneer Detects Sysplex Sysname xxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP013I** Pioneer Detects LPARNAME AS xxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP014I** Pioneer Detects Country Code of XX
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP015I** Pioneer Detects Job Wait Time Of xx Secs
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP015I** Pioneer Detects RECON wait time of xx Mins
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP020I** Pioneer Accepting Messages on xxx.xxx.xxx.xxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP020A** Pioneer Operator has Issued a Shutdown Command
Message-Type:	Action
Action Required:	Action
Conditions:	If Shut=Y
Output:	Console, SYSOUT

Message:	**IDMP020A** Pioneer has a Write Delay of <nnn> ms
Message-Type:	Action
Action Required:	Action
Conditions:	If WRITE_DELAY=nnn
Output:	Console, SYSOUT

Message:	**IDMP030I** Pioneer INITAPI was successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP031I** Pioneer GETCLIENTID was successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP032I** Pioneer CLIENT NAME/ID is xxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP033I** Pioneer CLIENT TASK is xxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP034I** Pioneer CREATE SOCKET was successful
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP035I** Pioneer BIND SOCKET was successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP036I** Pioneer Listening Address is xxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message: **IDMP037I** Pioneer Listening Address is xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Conditions: Unconditional

Output: Console, SYSOUT

Message: **IDMP038I** Pioneer Listen Socket Call was successful

Message-Type: Informational

Action Required: None

Conditions: Unconditional

Output: Console, SYSOUT

Message: **IDMP039I** Pioneer Read Socket Call was successful

Message-Type: Informational

Action Required: None

Conditions: Not Utilized

Output: Not Utilized

Message: **IDMP039I** Pioneer Write Socket Call was successful

Message-Type: Informational

Action Required: None

Conditions: Not Utilized

Output: Not Utilized

Message: **IDMP040I** Pioneer Translation was successful from-to xxxxxxxxxxxxxxxxxx. (ASCII-TO-EBCDIC) or (EBCDIC-TO-ASCII)

Message-Type: Informational

Action Required: None

Conditions: Not Utilized

Output: Not Utilized

Message:	**IDMP040E** Pioneer Translation was not successful from-to xxxxxxxxxxxxxxxxxx.(ASCII-TO-EBCDIC) or (EBCDIC-TO-ASCII)
Message-Type:	Error
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP041I** Pioneer Socket Accept was successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP041E** Pioneer Socket Accept was not successful RC: xxxxxxxx
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP048I** Pioneer LDAP Connection Timed out
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP049I** Pioneer Has Been Idle for 30 Mins
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP050A** Pioneer Closing IP Connection
Message-Type:	Action
Action Required:	Action
Conditions:	If Shut=Y
Output:	Console, SYSOUT

Message:	**IDMP051I** Pioneer Close Socket Call was Successful
Message-Type:	Informational
Action Required:	None
Conditions:	IF DEBUG ON
Output:	SYSOUT

Message:	**IDMP051I** Pioneer Close Socket Call was Successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP052I** Pioneer Shutdown Socket Call was Successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP053I** Pioneer MYRADMIN SAF call was Successful
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP054I** Pioneer Received TOPS Recon Request from LDAP
Message-Type:	Informational
Action Required:	None
Conditions:	IF Debug On
Output:	Console, SYSOUT

Message:	**IDMP055I** Pioneer Recon Processing Started
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	Console, SYSOUT

Message:	**IDMP056I** Pioneer Recon Processing Ended
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP057I** Pioneer Recon Processing Successful
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	Console, SYSOUT

Message:	**IDMP058I** Pioneer Recon Has Processed: xxxx Userids
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message: **IDMP058I** Pioneer Recon Total Processed: xxxxxx Userids
Message-Type: Informational
Action Required: None
Conditions: Not Utilized
Output: Not Utilized

Message: **IDMP070I** Pioneer xxxxxxxx Is Now Open
Message-Type: Informational
Action Required: None
Conditions: If Debug On
Output: Console, SYSOUT

Message: **IDMP071I** Pioneer xxxxxxxx Is Now Closed
Message-Type: Informational
Action Required: None
Conditions: Unconditional
Output: SYSOUT

Message: **IDMP071A** Pioneer has cleared the <filename> FILE
Message-Type: Action
Action Required: Action
Conditions: If Debug On
Output: SYSOUT

Message: **IDMP070E** Pioneer Could Not Open xxxxxxxx RC: xx
Message-Type: Error
Action Required: None
Conditions: Unconditional
Output: SYSOUT, Console

Message:	**IDMP070E** Pioneer Could Not Open xxxxxxxx RC: xx
Message-Type:	Error
Action Required:	None
Conditions:	If Debug On
Output:	SYSOUT

Message:	**IDMP080I** Pioneer Job Submitted to the Intrdr
Message-Type:	Informational
Action Required:	None
Conditions:	If Debug On
Output:	SYSOUT

Message:	**IDMP100I** Pioneer (IN) Msgs Processed is xxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT, Console

Message:	**IDMP100I** Pioneer (OUT) Msgs Processed is xxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP100I** Pioneer Message (READ) Bytes xxxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT, Console

Message:	**IDMP100I** Pioneer Message (WRITE) Bytes xxxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT, Console

Message:	**IDMP100I** Pioneer Debug Log Files Created <LOGFILES>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT, Console

Message:	**IDMP102I** Pioneer Terminating
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMP200E** Pioneer Startup Parameter Error xxxxxxxxxxxxxx
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMP200I** *Pioneer Paramater = <value> Value = <value>
Message-Type:	Informational
Action Required:	Unconditional
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP201I** Pioneer <Parmout> Status = Good
Message-Type:	Informational
Action Required:	Unconditional
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMP300I** *Debug* - xxxxxxxxxxxxxxxxxxxxxxx
Message-Type:	Action
Action Required:	None
Conditions:	If Debug On
Output:	DEBUGOUT

Message:	**IDMP400I** *Parms* - xxxxxxxxxxxxxxxxxxxxxxx
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP041E** *Parms* - "Message" "Status" "Text"
Message-Type:	Error
Action Required:	None
Conditions:	Unconditional
Output:	PARMOUT

Message:	**IDMP301I** Pioneer Dynamically Allocated Sysout Ok
Message-Type:	Informational
Action Required:	None
Conditions:	Not Utilized
Output:	Not Utilized

Message:	**IDMP303I** Pioneer Job Wait was modified by the operator to nnn secs
Message-Type:	Informational
Conditions:	If JWAIT= value
Output:	SYSOUT, Console

Message:	**IDMP304I** Pioneer Recon Wait time was modified by the operator to nnn secs
Message-Type:	Informational
Action Required:	None
Conditions:	If RWAIT = value
Output:	SYSOUT, Console

Message:	**IDMP305I** Pioneer Debugging was Turned <status>
Message-Type:	Error
Action Required:	None
Conditions:	If DEBG = Y/N
Output:	SYSOUT, Console

Message:	**IDMP306I** Pioneer Received Status Query and is Alive
Message-Type:	Informational
Action Required:	None
Conditions:	If HERT= Y
Output:	SYSOUT, Console

Message:	**IDMP500I** *AUDIT* - <Func> <CMD> <ACID> <STAT> <INFO>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	AUDITLOG

Message:	**IDMP500I** *HEADER* - <Func> <CMD> <ACID> <STAT> <INFO>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	AUDITLOG

Message:	**IDMP500I** Generic
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	AUDITLOG

Message:	**IDMP620I** *RADMIN* <value>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMP630I** *CLISTI* <value>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

Message:	**IDMP600I** *EXPMSG* <value>
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	EXPORTIN

Message:	**IDMP600I** Pioneer waiting for the LDAP to respond Timeouts = <value> times
Message-Type:	Informational
Action Required:	None
Conditions:	Unconditional
Output:	SYSOUT

I

Pioneer Searches – Initiated from the LDAP

Top-Secret searches for all ACIDS, DEPTS, DATASETS, and so on can be requested by the LDAP at anytime.

Following is an overview of the LDAP-Pioneer search process and how it works:

1. Backend (OIM) or equivalent software application requests a "SEARCH ALL". This request is forwarded to the LDAP.
2. LDAP sends the Request to Pioneer through TCPIP
3. Pioneer validates the quest. Reads the //RECONJCL ddname dataset, this is a skeleton of MVS JCL, during this read Pioneer inserts the Rexx clist name for the desired function. For example: A SEARCHALL is a "%SRCHUSR DSN=xxxxx.xxxxx.xx", the DSN= is the QUEUE_DSN specified in the Pioneer control file. This is a 1 track enqueue/dequeue file. Please do not allocate this file. The modified skeleton JCL is then submitted to MVS through the Intrdr for execution. At this point Pioneer goes into a temporary wait, Pioneer is SINGLE thread only one TCB.
4. The submitted JCL is a PGM=IKJEFT01 with a //SYSPROC pointing to the Distribution Clist library. A ddname of FILEOUT pointing to the Pioneer ddname file "RECONOUT". The REXX clist begins execution by trying to find the QUEUE_DSN=, if the file is there it is DELETED. During this process Pioneer is waiting. If the QUEUE_DSN= is not found then TSS LIST commands are issued and a file is built (DDNAME = FILEOUT). When the REXX finishes, the QUEUE_DSN= is built and the REXX clist finishes. During the wait, Pioneer waits and trys every 10 seconds to allocate the QUEUE_DSN= dataset as DISP=OLD. When Pioneer can do this, it reads the file and sends it back to the LDAP. After all the data has been sent through Socket-writes to the LDAP, Pioneer deletes the records from the input file.

J

Pioneer and Voyager LONG_FDTNAME=Y Processing

This appendix describes the Pioneer and Voyager LONG_FDTNAME=Y Processing. The Pioneer and/or Voyager agent, after receiving a TSS LIST request as a part of its internal logic, issues a TSS LIST for appropriate Top-Secret ACID.

When the list request is issued, Pioneer and/or Voyager will issue a @PSCRCHUSR acid dsn for Pioneer or @VSRCHUSR acid dsn through module IDFISCMD to IBM's System Rexx.

The new module uses MGCRE macro to issue this request. AXR (System Rexx) queues up the request and searches its REXXLIBs for the Rexx clist. The clists perform a TSO "LISTDS" for the dsname that is passed to System Rexx. If the dataset is found it is deleted.

A TSS LIST for the acid is then performed and the dsn is built. During this period, Pioneer and or Voyager will wait until it can allocate the dataset as OLD. When able to allocate Pioneer and/or Voyager will build messages for the LDAP, convert to ASCII, encrypt them and then issue a write socket.

The DSN specified must be unique for Pioneer and Voyager. The AXR STC (Started Task) must be able to update and delete these datasets.

Specify the control parameter LONG_FTDNAMES=Y when DSN=<YOURHLQ.DATASERNAME>. The YOURHLQ.DATASERNAME must be unique for each STC. If this feature is not required, code the control parameter LONG_FTDNAMES=N. LONG_FDT=Y indicates that the connector will support user-defined fields greater than 255 bytes.

They are also preallocated by the PSRCHUSR and VSRCHUSR Rexx clists in the REXXlib specified for System Rexx.

K

Mainframe Language Environment Runtime Options

If the following settings are not properly set, they can cause random S806 or S0C4 conditions.

1. Add the following CEEOPTS DD to your PIONEER and or VOYAGER Task (or other modules through STC/JCL) as needed.

   Example (this may vary by site requirements):

   ```
   //CEEOPTS DD DISP=SHR,
   //DSN=&SYSPLEX.OIDM.VOYAGER.CONTROL.PARMLIB(CEEPRM00)
   ```

2. Where the CEEPRM00 PDS member contains:

   a. RPTOPT(ON)

   b. RPTSTG(ON)

3. When you run the offending STC/JCL again you will get a list of the options in affect.

4. Compare the output of the current JES LOG and look for one of the following literals, so one may review the current options in place.

   a. "LAST WHERE SET"

   b. "IBM-supplied default"

   c. "ALL31"

5. Note that all LE options should all be reviewed (not only ALL31) as noted in step 8 of this section.

6. The options can be overridden within the CEEOPTS DD through the CEEPRM00 PDS member (or site specific implementation), as follows:

   - Where CEEPRM00
   - ALL31(ON)
   - RPTOPT(ON)
   - RPTSTG(ON)
   - STACK(128K,128K,ANYWHERE,KEEP,512K,512K)

7. When the anomaly is addressed, the RPT* lines can be removed, if desired:

   - Where CEEPRM00
   - ALL31(ON)

- STACK(128K,128K,ANYWHERE,KEEP,512K,512K)

8. Customizing Language Environment run time options Z/OS Language Environment Customization: Info gathered from IBM Manual # SA22-7564-13.

Table K–1 lists Language Environment run time options, defaults and recommendations.

Table K–1 Language Environment Run Time Options, Defaults and Recommendations

Option	Default	Recommended	IDF's
ABPERC	NONE	NONE	NONE
ABTERMENC	ABEND	ABEND	ABEND
AIXBLD	OFF	OFF	OFF
ALL31	ON	ON	ON
ANYHEAP	16K,8K,ANY,FREE	16K,8K,ANY,FREE	16K,8K,ANY,FREE
ARGPARSE	ARGPARSE	ARGPARSE	ARGPARSE
AUTOTASK	NOAUTOTASK	NOAUTOTASK	NOAUTOTASK
BELOWHEAP	8K,4K,FREE	8K,4K,FREE	8K,4K,FREE
CBLOPTS	ON	ON	ON
CBLPSHPOP	ON	N/A	ON
CBLQDA	OFF	OFF	OFF
CEEDUMP	60,SYSOUT=*,FREE-END,SPIN-UNALLOC	60,SYSOUT=*,FREE-END,SPIN-UNALLOC	60,SYSOUT=*,FREE-END,SPIN-UNALLOC
CHECK	ON	ON	ON
COUNTRY	US	User defined	US
DEBUG	OFF	OFF	OFF
DEPTHCONDLMT	10	0	10
DYNDMP	*USERID,NODYNAMIC,TDUMP	*USERID,NODYNAMIC,TDUMP	*USERID,NODYNAMIC,TDUMP
ENV	No default	User default	No default
ENVAR	"	"	"
ERRCOUNT	0	0	0
ERRUNIT	6	6	6
EXECOPS	EXECOPS	EXECOPS	EXECOPS
FILEHIST	ON	ON	ON
FILETAG	NOAUTOCVT, NOAUTOTAG	NOAUTOCVT, NOAUTOTAG	NOAUTOCVT, NOAUTOTAG
HEAP	32K,32K,ANY,KEEP,8K,4K	32K,32K,ANY,KEEP,8K,4K	32K,32K,ANY,KEEP,8K,4K
HEAP64	1M,1M,KEEP,32K,32K,KEEP,4k,4K,FREE	N/A	N/A
STACK	128K,128K,ANY,KEEP,512K,128K	128K,128K,ANY,KEEP,512K,128K	128K,128K,ANY,KEEP,512K,128K

There are many more run time options that are not applicable to this situation.

Index