

Oracle® Identity Manager

Connector Guide for CA ACF2 Advanced



9.1.0.2.0
F14866-06

ORACLE®

Oracle Identity Manager Connector Guide for CA ACF2 Advanced, 9.1.0.2.0

F14866-06

Copyright © 2020, 2023, Oracle and/or its affiliates.

Primary Author: Maya Chakrapani

Contributors: Amol Datar

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, and MySQL are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	ix
Documentation Accessibility	ix
Related Documents	ix
Conventions	ix

What's New in Oracle Identity Manager Connector for CA ACF2?

Software Updates	xi
Documentation-Specific Updates	xii

1 About the Connector

Introduction to the Connector	1-1
Certified Components	1-2
Certified Languages	1-2
Connector Architecture	1-3
Connector Components	1-3
Connector Operations	1-4
Full Reconciliation Process	1-4
Incremental Reconciliation Process	1-5
Provisioning Process	1-6
Use Cases Supported by the CA ACF2 Connector	1-8
Features of the Connector	1-9
Target Resource Reconciliation	1-9
Full and Incremental Reconciliation	1-9
Limited (Filtered) Reconciliation	1-9
Encrypted Communication Between the Target System and Oracle Identity Manager	1-10
High Availability	1-10
Connector Objects Used During Reconciliation and Provisioning	1-11
Supported Functions for Reconciliation	1-11
Supported Functions for Provisioning	1-11
User Attributes for Target Resource Reconciliation and Provisioning	1-12

Resource Rule Attributes for Target Resource Provisioning	1-18
Access Rule Attributes for Target Resource Provisioning	1-18
Privilege Attribute for Target Resource Reconciliation and Provisioning	1-19
Reconciliation Rule	1-19
Reconciliation Action Rules	1-20
Lookup Definitions Used for Provisioning and Reconciliation	1-21

2 Deploying the Agents of the CA ACF2 Connector on the Target System

Deployment Requirements	2-1
Installing the Mainframe Agents	2-3
Configuring the Mainframe Agents	2-7
Configuring the Provisioning Agent	2-7
Configuring the Reconciliation Agent	2-8
Activating and Deactivating Reconciliation Exits	2-10
Activating Reconciliation Exits	2-10
Deactivating Reconciliation Exits	2-10
Operator Interface for Mainframe Agents	2-10
Provisioning Agent Commands	2-11
About Reconciliation Agent Commands	2-11
Uninstalling the Mainframe Agents	2-12

3 Installing and Configuring the LDAP Gateway

System Requirements	3-1
LDAP Gateway Concepts	3-2
About Encrypting Data	3-2
About Caching Layer	3-3
About Scheduled Recon Utility	3-4
About Parsing Grammar Protocol 1.0	3-5
Files and Directories that Comprise the LDAP Gateway	3-9
Installing the LDAP Gateway	3-10
Configuring the LDAP Gateway	3-12
Creating a Connector Configuration	3-12
Editing the System Administrator Credentials for Target	3-13
Configuring the LDAP Gateway with Multiple Connectors	3-14
Overriding the System Configuration	3-15
Configuring the Adapter	3-16
Configuring Windows Service	3-19
Installing and Configuring the Windows Service for the LDAP Gateway	3-19
Uninstalling the Windows Service for the LDAP Gateway	3-19

	Configuring Memory Pool Settings	3-20
	Starting the LDAP Gateway	3-20
4	Connector Deployment on Oracle Identity Manager	
	Files and Directories in the CA_ACF2_Connector.zip	4-1
	Running the Connector Installer	4-2
	Configuring the IT Resource	4-3
	Configuring Oracle Identity Manager	4-6
	Creating and Activating a Sandbox	4-6
	Creating a New UI Form	4-6
	Creating an Application Instance	4-6
	Publishing a Sandbox	4-6
	Updating an Existing Application Instance with a New Form	4-7
	Enabling Logging	4-7
5	Using the Connector	
	Guidelines on Using the Connector	5-1
	Performing Full Reconciliation	5-1
	Performing Filtered (Limited) Reconciliation	5-4
	Reconciling Internal LDAP Users to Oracle Identity Manager	5-5
	Reconciling Deleted Users to Oracle Identity Manager	5-7
	Configuring Resource and Access Rule PrePopulation Scheduled Tasks	5-8
	Reconciling Internal LDAP Users to Oracle Identity Manager	5-10
	Uninstalling the Connector	5-12
6	Extending the Functionality of the Connector	
	Adding New Attributes for Target Resource Reconciliation	6-1
	Adding Custom Fields for Full Reconciliation	6-2
	Adding Custom Fields to Oracle Identity Manager	6-2
	Adding New Attributes for Provisioning	6-3
	Removing Attributes Mapped for Target Resource Reconciliation and Provisioning	6-5
	Configuring the Connector for Provisioning to Multiple Installations of the Target System	6-5
7	Troubleshooting	
A	Files and Directories in the ACF2 Connector Installation Media	

B Reconciliation Agent (Voyager) Messages

C Provisioning Agent (Pioneer) Messages

D Authorized Libraries

E Relationship between the Pioneer (DDs), Voyager (DDs) and the INDDs

List of Figures

1-1	Incremental Reconciliation Process	1-5
1-2	Provisioning Process	1-7

List of Tables

1-1	Certified Components	1-2
1-2	Supported Functions for Provisioning	1-12
1-3	User Attributes for Target Resource Reconciliation and Provisioning	1-12
1-4	Resource Rule Attribute Mappings	1-18
1-5	Access Rule Attribute Mappings	1-19
1-6	Privilege Attribute Mapping	1-19
1-7	Reconciliation Action Rules	1-20
1-8	Lookup Definition and Descriptions	1-21
2-1	Deployment Requirements	2-1
2-2	Installation Placeholders	2-5
2-3	Job Streams to Execute	2-6
2-4	Provisioning Agent Parameters	2-7
2-5	Reconciliation Agent Parameters	2-8
2-6	Provisioning Agent Commands	2-11
2-7	Reconciliation Agent Commands	2-11
3-1	Files and Directories that Comprise the Gateway	3-9
4-1	Files and Directories in the CA_ACF2_Connector.zip	4-1
4-2	IT Resource Parameter	4-4
4-3	Logger Parameters	4-8
5-1	Attributes of the Reconcile All Users Scheduled Task	5-2
5-2	Attributes of the Reconcile LDAP Users Scheduled Task	5-6
5-3	Attributes of the Deleted User Reconciliation to OIM Scheduled Task	5-8
5-4	Attributes of the FindAllAccessRules and FindAllResourceRules Scheduled Tasks	5-9
5-5	Attributes of the Reconcile LDAP Users Scheduled Task	5-11
7-1	Troubleshooting Tips	7-1
7-2	Three Options Settings and their Effects	7-3
A-1	Files and Directories on the Installation Media	A-1
E-1	Relationship between the Pioneer (DDs) and the INDDs in CREATDSN Member	E-1
E-2	Relationship between the Voyager (DDs) and the INDDs in CREATDSN Member	E-2
E-3	Purpose of the Pioneer (DDs)	E-2

Preface

This guide provides information about integrating Oracle Identity Manager with CA ACF2.

Audience

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

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 Governance 12.2.1.4.0, visit the following Oracle Help Center page:

<https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.4/index.html>

For information about installing and using Oracle Identity Governance 12.2.1.3.0, visit the following Oracle Help Center page:

<https://docs.oracle.com/en/middleware/idm/identity-governance/12.2.1.3/index.html>

For information about Oracle Identity Governance Connectors 12.2.1.3.0 documentation, visit the following Oracle Help Center page:

<https://docs.oracle.com/en/middleware/idm/identity-governance-connectors/12.2.1.3/index.html>

For information about Oracle Identity Manager Connectors 11.1.1 documentation, visit the following Oracle Help Center page:

http://docs.oracle.com/cd/E22999_01/index.htm

Conventions

The following text conventions are used in this document:

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

What's New in Oracle Identity Manager Connector for CA ACF2?

These are the updates made to the software and documentation for release 9.1.0.2.0 of the Connector Guide for CA ACF2 Advanced.

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

- [Software Updates](#)
These include updates made to the connector software.
- [Documentation-Specific Updates](#)
These include the major changes that are made to the connector documentation. These changes are not related to software updates.

Software Updates

These are the updates made to the connector software.

Software Updates in Release 9.1.0.2.0

The following are software updates in release 9.1.0.2.0:

- [Support for New Oracle Identity Governance Release](#)
- [Resolved Issues in Release 9.1.0.2.0](#)

Support for New Oracle Identity Governance Release

From this release onward, you can install and use the connector with Oracle Identity Governance 12c PS4 (12.2.1.4.0).

See [Certified Components](#) for the full list of certified Oracle Identity Governance releases.

Resolved Issues in Release 9.1.0.2.0

The following table lists the issues resolved in release 9.1.0.2.0:

Bug Number	Issue	Resolution
31216418	The name value in the target system was incorrectly formatted when there was a space character between Lastname and Firstname.	This issue has been resolved.

Software Updates in Release 9.1.0.1.0

The following table lists the issues resolved in release 9.1.0.1.0:

Bug Number	Issue	Resolution
31030283	After a Create User provisioning operation, the name value in the target system was being formatted incorrectly. For example, the name value being stored in the target system was enclosed within single quotation marks (').	This issue has been resolved.

Software Updates in Release 9.1.0.0.0

The following are the software updates in release 9.1.0.0.0:

- **Support for New Oracle Identity Manager Releases**

From this release onward, the connector can be installed and used on Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0) and Oracle Identity Governance release 12.2.1.3.0. If you are using Oracle Identity Governance release 12.2.1.3.0, then ensure to download and apply the 28682376 and 29133050 mandatory patches from [My Oracle Support](#).

See [Certified Components](#) for the full list of certified Oracle Identity Manager releases.

- **Support for New Target System Versions**

From this release onward, you can install and use the connector with CA ACF2 on R15 and R16.

- **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.

- **End of Life Support for Realtime Reconciliation from the Gateway to Oracle Identity Manager**

From this release onward, the connector no longer supports real-time reconciliation to Oracle Identity Manager from the gateway. The scheduled tasks `ACF2 Reconcile LDAP Users` can be configured to run periodically to fetch data from the gateway. Voyager agent still send real-time incremental events to gateway.

- **Support for High Availability and Disaster Recovery in the LDAP Gateway**

From this release onward, the LDAP gateway supports high availability and disaster recovery when you use OpenDS as the backend.

Documentation-Specific Updates

These are the updates made to the connector documentation.

Documentation-Specific Updates in Release 9.1.0.1.0 and 9.1.0.2.0

The following documentation-specific update has been made in revision "04" of this guide:

The Target system row of [Certified Components](#) has been updated to include support for IBM z/OS 2.4.

The following documentation-specific update has been made in revision "03" of this guide:

The "Oracle Identity Governance or Oracle Identity Manager" row of [Certified Components](#) has been updated to include support for Oracle Identity Governance 12c (12.2.1.4.0).

Documentation-Specific Updates in Release 9.1.0.0.0

The following documentation-specific updates have been made in revision "02" of this guide:

- The "JDK" and "LDAP Gateway" rows of [Certified Components](#) have been updated.
- The following topics have been updated to clarify the encryption requirement for the connector:
 - The "Infrastructure requirement for the message transport layer between Oracle Identity Manager and the mainframe environment" row of [Certified Components](#)
 - Description of the Message Transport Layer component in [Connector Components](#)
 - [Encrypted Communication Between the Target System and Oracle Identity Manager](#)
 - The "Message Transport Layer" row of [Deployment Requirements](#)
- The "idfbackendContext", "idfBackendDn", "idfBackendPassword", "idfPrincipalPwd", "idfServerHost", and "idfSsl" rows have been updated in [Configuring the IT Resource](#).
- [Configuring Memory Pool Settings](#) has been added.
- Minor editorial corrections have been made.

The following documentation-specific update has been made in revision "01" of this guide:

This is the first release of this connector in the 9.1.0.x release track. Therefore, there are no documentation-specific updates in this release.

1

About the Connector

This chapter introduces the CA ACF2 connector.

This chapter is divided into the following sections:

- [Introduction to the Connector](#)
- [Certified Components](#)
- [Certified Languages](#)
- [Connector Architecture](#)
- [Use Cases Supported by the CA ACF2 Connector](#)
- [Features of the Connector](#)
- [Connector Objects Used During Reconciliation and Provisioning](#)

Introduction to the Connector

Oracle Identity Manager connectors are used to integrate Oracle Identity Manager with external, identity-aware applications.

Oracle Identity Manager automates access rights management, security, and provisioning of IT resources. This guide discusses the connector that enables you to use CA ACF2 as a managed (target) resource of identity data for Oracle Identity Manager.

The advanced connector for CA ACF2 provides a native interface between Oracle Identity Manager and CA ACF2 installed on an IBM z/OS mainframe.

In the account management (target resource) mode of the connector, information about users 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.

If you configure CA ACF2 as a target resource, then user profiles on CA ACF2 correspond to accounts or resources assigned to OIM users.

Certified Components

These are the software components and their versions required for installing and using the CA ACF2 connector.

Table 1-1 Certified Components

Component	Requirement
Oracle Identity Governance or Oracle Identity Manager	<p>You can use one of the following releases:</p> <ul style="list-style-type: none"> Oracle Identity Governance 12c PS4 (12.2.1.4.0) Oracle Identity Governance 12c PS3 (12.2.1.3.0) with the following mandatory patches: <ul style="list-style-type: none"> 28682376 29133050 Oracle Identity Manager 11g Release 2 PS3 (11.1.2.3.0)
Target system	CA ACF2 R15 or R16 running on IBM z/OS 2.2, 2.3, 2.4, or 2.5
JDK	<p>The JDK version can be one of the following:</p> <ul style="list-style-type: none"> For Oracle Identity Governance release 12.2.1.3.0 or later, use JDK 1.8.0_131+ . For Oracle Identity Manager release 11.1.2.x or later, use JDK 1.6 update 31 or later.
LDAP Gateway	<p>The computer hosting the LDAP Gateway must run the following software:</p> <ul style="list-style-type: none"> Operating system: Microsoft Windows Server 2012, or Red Hat Enterprise Linux 7 (64-bit) Oracle Java JRE 1.8 or 1.7
Infrastructure Requirements: Message transport layer between the Oracle Identity Manager and the mainframe environment	TCP/IP

Certified Languages

These are the languages that the connector supports.

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

- Portuguese
- Spanish

Connector Architecture

The connector architecture is described in the following sections:

- [Connector Components](#)
- [Connector Operations](#)

Connector Components

The CA ACF2 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 converted into native commands for CA ACF2, encrypted using AES-128 encryption, and then sent to the Provisioning Agent. The response, which is also native to CA ACF2, 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.
- **Provisioning Agent (Pioneer):** The Provisioning Agent, running as an IBM z/OS STC (Started Task), is a mainframe component. It receives native mainframe CA ACF2 provisioning commands from the LDAP Gateway. These requests are decrypted, converted from ASCII to EBCDIC, passed to CA ACF2 through the standard RACF Sub System Interface API, and then posted to the CA ACF2 database. The response is parsed and returned to the LDAP Gateway.

 **Note:**

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

- **Reconciliation Agent (Voyager):** The Reconciliation Agent captures mainframe events by using exits, which are programs run after events in CA ACF2 are processed. These events include the ones generated at the TSO logins, the command prompt, batch jobs, and other native events. The Reconciliation Agent captures these events, transforms them into 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:** This connector supports a message transport layer by using the TCP/IP protocol, which is functionally similar to proprietary message transport layer protocols. In addition, the connector provides AES encryption for messages sent and received through the transport layer.

The AES encryption is performed using 128-bit cryptographic keys. In addition, Encryption and Decryption programs are supplied in the Distribution Load Library. The encryption or decryption does not require any network software or hardware.

Connector Operations

These are the operations that the connector performs.

This section provides an overview of the following processes:

- [Full Reconciliation Process](#)
- [Incremental Reconciliation Process](#)
- [Provisioning Process](#)

Full Reconciliation Process

Full reconciliation involves fetching all existing user profile data from the mainframe to Oracle Identity Manager.

The following is a summary of the full reconciliation process:



Note:

See [Performing Full Reconciliation](#) for detailed instructions of the full reconciliation process.

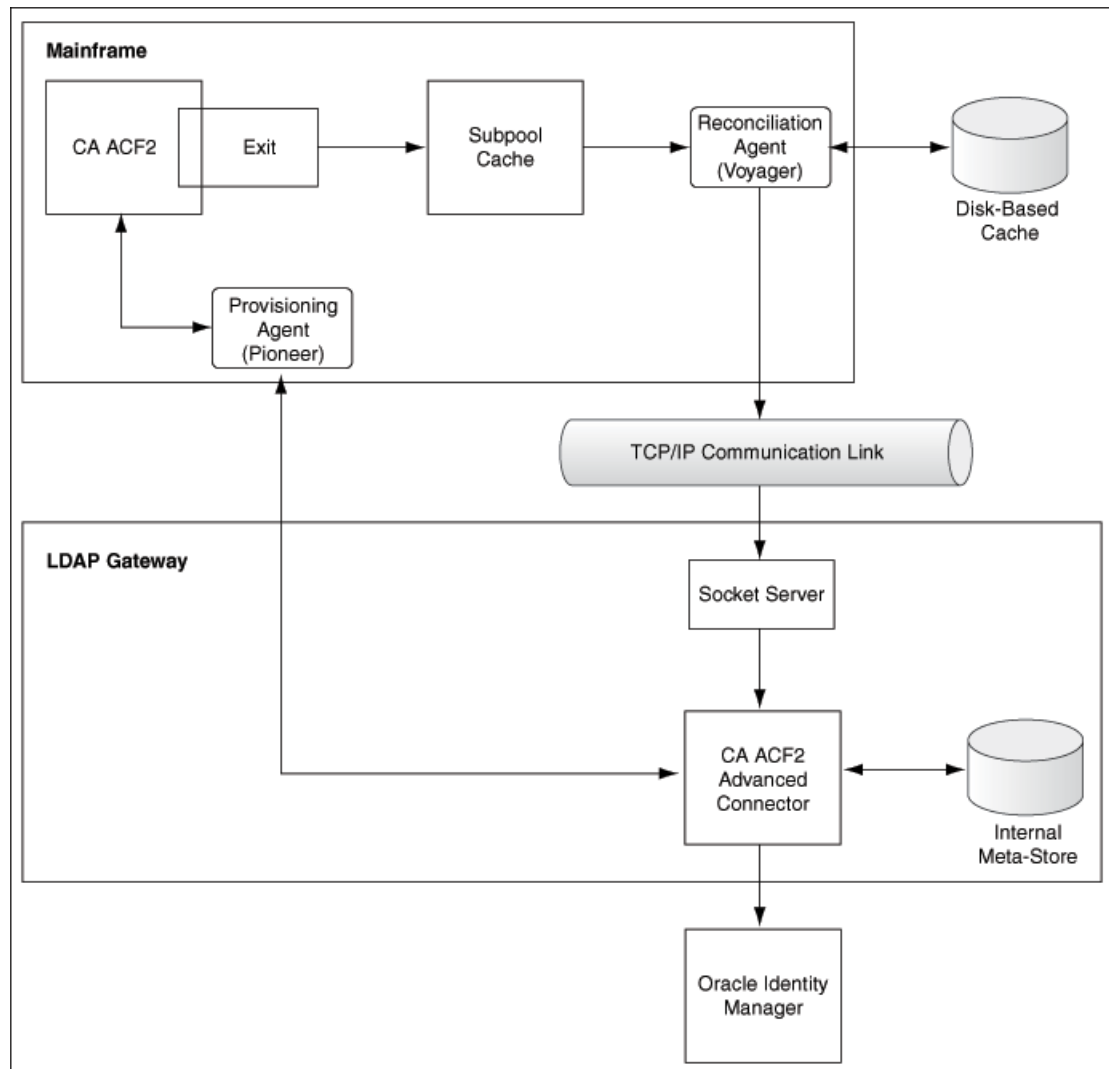
1. You specify the full reconciliation configuration in the ACF2 Reconcile All Users scheduled task.
2. In the scheduled task form UsersList property, you enter a list of user IDs of the user profiles that you want to reconcile. If no users are specified, then all existing users on the target system will be reconciled.
3. You set a start time for the task and run the scheduled task. The task sends the list of user IDs to the LDAP Gateway.
4. The LDAP Gateway encrypts the list of user IDs and then sends it to the Provisioning Agent on the mainframe.
5. You run the scheduled task. The task sends a search request to the LDAP Gateway.
6. The LDAP Gateway encrypts the search request and then sends it to the Provisioning Agent on the mainframe.
7. The Provisioning Agent encrypts the user profile data received from ACF2 and then passes this data to the LDAP Gateway.
8. The LDAP Gateway decrypts the user profile data and passes it to Oracle Identity Manager.
9. If you configure the target system as a target resource, then this user profile data is converted into accounts or resources for OIM Users.

Incremental Reconciliation Process

In incremental reconciliation, only records that are added or modified after the last reconciliation run are fetched into Oracle Identity Manager.

Incremental reconciliation is initiated by one of the exits that work in conjunction with the Reconciliation Agent. [Figure 1-1](#) shows the flow of data during this form of reconciliation.

Figure 1-1 Incremental Reconciliation Process



The following is a summary of the incremental reconciliation process:

1. Incremental reconciliation begins when a user is created, updated, or deleted on CA ACF2. This event might take place either directly on the mainframe or in response to a provisioning operation on Oracle Identity Manager.
2. The Reconciliation Agent gathers data captured by one of three CA ACF2 exits: LIDPOST, NEWPXIT, or EXPPXIT. The exit detects the event and sends a message

containing user data to Subpool 231 (cache). This message contains the minimum number of data items, such as the user ID and password, required to reconcile the event.

3. The Reconciliation Agent polls Subpool 231. When it finds a message in the subpool, it reads the message into its buffer. This frees up the subpool entry.
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.
- As mentioned in Step 2, the message sent by the Reconciliation Agent contains only a minimum amount of data. The LDAP Gateway sends a request to the Provisioning Agent to fetch the remaining user data from the target system.

 **Note:**

Messages sent to the LDAP Gateway are encrypted using AES-128 encryption.

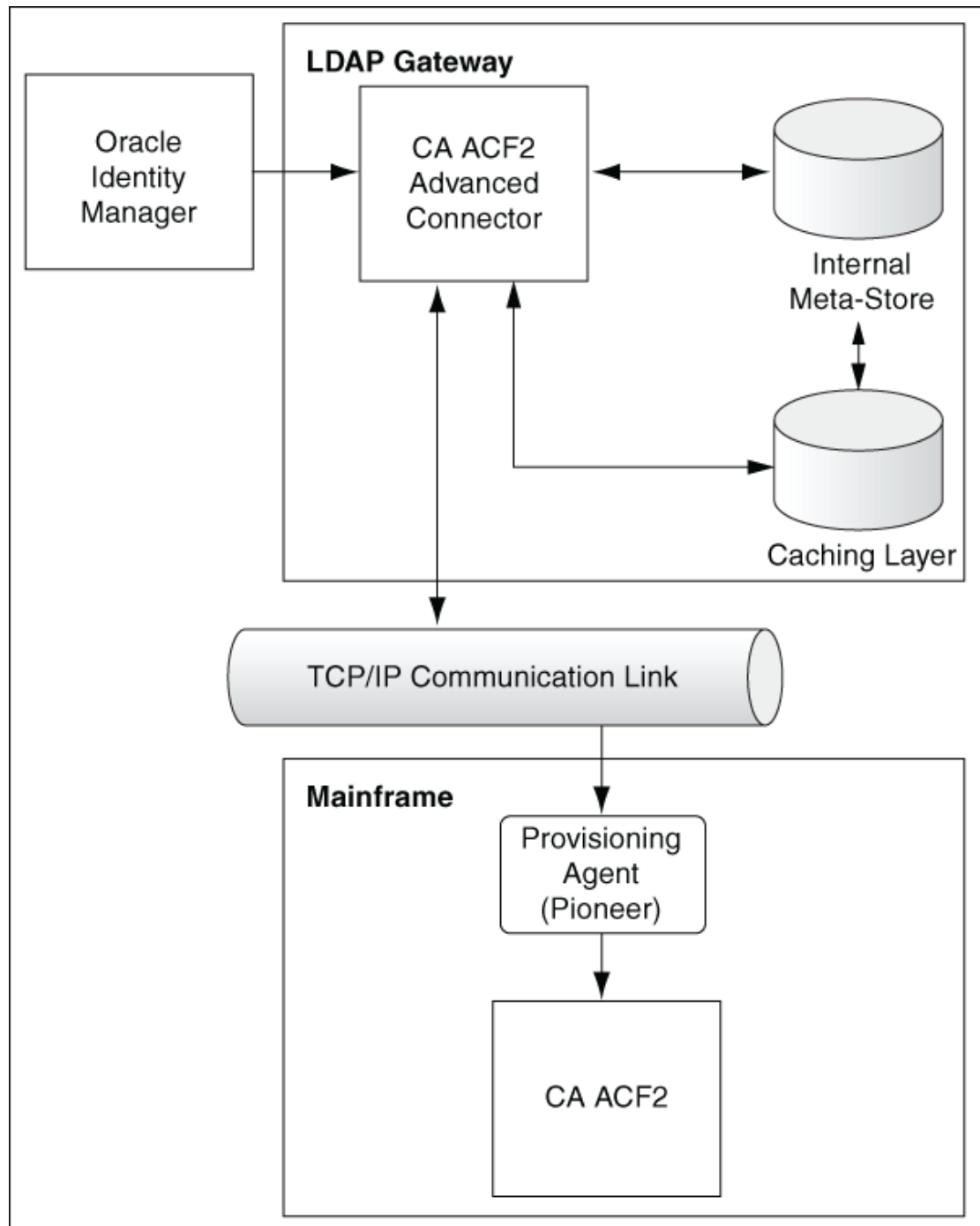
5. The LDAP Gateway stores the events received from Reconciliation Agent (Voyager) in its backend, also known as persistent storage, if `_internalEnt_` is set to `true` in the connector properties file in the Gateway.
6. OIM then fetches these incremental events using `ACF2 Reconcile All Ldap Users` scheduled task which is communicated to LDAP's backend.

Provisioning Process

Provisioning involves creating or modifying a user's data on the target system through Oracle Identity Manager.

[Figure 1-2](#) shows the flow of data during provisioning.

Figure 1-2 Provisioning Process



The following is a summary of the provisioning process:

1. Provisioning data is sent from Oracle Identity Manager to the LDAP Gateway.
2. The LDAP Gateway converts the provisioning data into mainframe commands, encrypts the commands, and then sends them to the mainframe over TCP/IP
3. The Provisioning Agent installed on the mainframe decrypts the commands and then runs them on the mainframe.

4. The Provisioning Agent sends the output of the commands 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.

Use Cases Supported by the CA ACF2 Connector

Large enterprises rely on mainframe systems for critical applications. The CA ACF2 security system is used to secure these mainframe systems. The following are some of the most common scenarios in which this connector can be used:

- User Management

Creating and managing CA ACF2 users is traditionally done by the mainframe security team using native command line tools. Using the Oracle Identity Manager CA ACF2 connector, you can perform the CA ACF2 user management operations from Oracle Identity Manager. Joiner, mover, and leaver processes can be automated, and a user's ACF2 LID can be created by the Oracle Identity Manager team with little or minimal knowledge of underlying CA ACF2 commands. The following are some use cases for user management:

 - Create user
 - Update user
 - Reset password
 - Enable or disable user
 - Add or remove a user from the ACF2 Access Rule
 - Add or remove a user from the ACF2 Resource Rule
- Password Management

Password reset requests are the highest contributors to helpdesk tickets where employees forget their password and call helpdesk. Using the Oracle Identity Manager CA ACF2 connector, employees can login to Oracle Identity Manager and perform a self-service password reset. This saves time and cost for the helpdesk team. Some enterprises also have password reset policies which can be automated using this connector through Oracle Identity Manager.
- Access to mainframe datasets

Mainframe datasets are like files and folders on an operating system. CA ACF2 users need access to these datasets to perform their job. Enterprises using CA ACF2 use CA ACF2 Access Rules to protect these datasets. Using Oracle Identity Manager CA ACF2 connector, users can request for Access Rules, and, if approved by their manager, the Oracle Identity Manager CA ACF2 connector will provision the user's access to the access rule. This increases employee productivity.
- Access to mainframe resources

In addition to datasets, mainframe system has generic resources, for example TSO, CICS. These resources are protected using CA ACF2 Resource Rules. Using the Oracle Identity Manager CA ACF2 connector, users can request for resource rules, and, if approved by their manager, the Oracle Identity Manager CA ACF2 connector will provision user's access to the resource rule.
- LOGON ID Reconciliation

Oracle Identity Manager CA ACF2 connector supports full reconciliation of ACF2 LOGON IDs. The LOGIN ID attributes are reconciled based on their configuration.

- Real time reconciliation for users

Oracle Identity Manager CA ACF2 connector also supports real-time reconciliation for users. If any CA ACF2 LID is created or updated natively in CA ACF2, then that change is detected by the Voyager component of the connector, and the changed user event is sent to the gateway persistence backend (dc=system,dc=backend). This can further be reconciled in Oracle Identity Manager using the CA ACF2 Reconcile LDAP Users task. This task can be configured to run in pre-defined intervals.

Features of the Connector

The following are features of the connector:

- [Target Resource Reconciliation](#)
- [Full and Incremental Reconciliation](#)
- [Limited \(Filtered\) Reconciliation](#)
- [Encrypted Communication Between the Target System and Oracle Identity Manager](#)
- [High Availability](#)

Target Resource Reconciliation

Target resource reconciliation involves fetching data about newly created or modified users on the target system and using this data to add or modify resources assigned to OIM users.

You can use the connector to configure CA ACF2 as a target resource of Oracle Identity Manager.

Full and Incremental Reconciliation

Full reconciliation involves reconciling all existing user records from the target system into Oracle Identity Manager, while in incremental reconciliation, only the records created or modified after the latest date/timestamp the last reconciliation was run are considered for reconciliation.

After you deploy the connector, you 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. OIM can fetch incremental events from the LDAP Backend using the task `ACF2 Reconcile All LDAP Users`. See [Reconciling Internal LDAP Users to Oracle Identity Manager](#) and [Performing Full Reconciliation](#) for more details. You can perform a full reconciliation run at any time.

Limited (Filtered) Reconciliation

You can reconcile records from the target system based on a specified filter criterion.

ACF2 Connector offers the following filtered reconciliation features at various levels:

- Logon ID filtering - The Scheduled Task `ACF2 Reconcile All Users` provides this feature with the parameter `UserLists`. For more information, see [Performing Full Reconciliation](#).


- Attribute level filtering - The scheduled task `ACF2 Reconcile All Users` provides this feature. For more information, see [Performing Filtered \(Limited\) Reconciliation](#).
- Filtering at agent level - Pioneer and Voyager provide this additional filtering feature. For more information, see [Table 2-4](#) and [Table 2-5](#).

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 and Provisioning Agents on the Mainframe. This encryption is taken care by the Mainframe agents.

High Availability

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**
 - The Reconciliation Agent stops sending messages (event data) to the LDAP Gateway.
 - Messages that are not sent are stored in the subpool cache.
-  **Note:**

The subpool cache cannot grow beyond the allocated limit. If the LDAP Gateway does not start responding before the allocated limit is reached, then new messages that come in are lost.
- 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**
 - Event data is sent to the subpool cache.
 - When the Reconciliation Agent is brought back online, it reads data from the subpool cache and then sends messages to the LDAP Gateway.
 - **Scenario 3: The LDAP Gateway is running and the mainframe stops responding**
 - Messages that are in the subpool cache are written to disk.
 - When the mainframe is brought back online, event data written to disk is again stored in the subpool cache.
 - The Reconciliation Agent reads data from the subpool cache and then sends messages to the LDAP Gateway.

- **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, messages in the AES-encrypted file are not affected and can be recovered.

Connector Objects Used During Reconciliation and Provisioning

As discussed in one of the earlier sections, target resource reconciliation involves fetching data about newly created or modified users on the target system and using this data to add or modify resources assigned to OIM Users. Provisioning involves creating or modifying account data on the target system through Oracle Identity Manager.

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

- [Supported Functions for Reconciliation](#)
- [Supported Functions for Provisioning](#)
- [User Attributes for Target Resource Reconciliation and Provisioning](#)
- [Reconciliation Rule](#)
- [Reconciliation Action Rules](#)
- [Lookup Definitions Used for Provisioning and Reconciliation](#)

Supported Functions for Reconciliation

These are the list of operations that the connector supports for your mainframe.

The connector supports reconciliation of user profile data from the following operations:

- Create user
- Modify user
- Change password
- Disable user
- Delete user
- Enable user
- Grant user access to privileges

Supported Functions for Provisioning

These are the list of operations that the connector supports for your target system.

[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 login ID record on CA ACF2	INSERT
Modify user	Modifies login ID record information on CA ACF2	CHANGE
Change password	Changes user password on CA ACF2 in response to password changes made on Oracle Identity Manager through user self-service.	CHANGE
Reset password	Resets user password on CA ACF2 The passwords are reset by the administrator.	CHANGE
Disable user	Disables user on CA ACF2	CHANGE
Enable user	Enables user on CA ACF2	CHANGE
Delete user	Removes user from CA ACF2	DELETE
Grant user access to rule	Creates or modifies a CA ACF2 resource or access rule for the CA ACF2 user	SET RULE
Grant user access to privileges (TSO)	Provides user access to CA ACF2 security fields (including custom fields)	CHANGE
Grant user access to privileges (CICS)	Provides user access to CA ACF2 CICS login ID record fields	CHANGE

User Attributes for Target Resource Reconciliation and Provisioning

[Table 1-3](#) lists attribute mappings between CA ACF2 and Oracle Identity Manager for target resource reconciliation and provisioning. The OnBoardAcf2User and ModifyAcf2User adapters are used for the Create User and Modify User provisioning operations, respectively.

Table 1-3 User Attributes for Target Resource Reconciliation and Provisioning

OIM Form	ACF2 Attribute	LDAP Attribute	Attribute Type	Description
USER_ID	UID	uid	24 characters	User login ID
FULL_NAME	NAME	cn	20 characters	User full name
DEFAULT_GROUP	GROUP	group	8 characters	Restriction group
USER_PASSWORD	PASSWORD	userPassword	8 to 128 characters	Password used to login
PWD_EXPIRE	PSWD-EXP	passwordExpire	bit field	Date the user password expires

Table 1-3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Form	ACF2 Attribute	LDAP Attribute	Attribute Type	Description
ACTIVE_DATE	ACTIVE	activeDate	4-byte binary	Active date privilege
EXPIRE_DATE	EXPIRE	expireDate	4-byte binary	Expire date privilege
TSO_DFTPFX	DFT-PFX	omvUid	8 characters. however, the last character is reserved	OMV UID tsoDftPfx DFT-PFX TSO DFT-PFX
TSO_ACCTNUM	TSOACCT	tsoAcctNum	40 characters	Default TSO account number on the TSO/E logon panel
TSO_PROC	TSOPROC	tsoProc	8 characters	Default logon procedure on the TSO/E logon panel
TSO_SIZE	TSORGN	tsoSize	2-byte binary	Minimum region size if not requested at logon
TSO_UNIT	TSOUNIT	tsoUnit	8 characters	Default UNIT name for allocations
TSO_MAXSIZE	TSOSIZE	tsoMaxSize	2-byte binary	The maximum region size the user can request at logon
TSO_PERF	TSOPERF	tsoPerf	1-byte binary	Indicates the user's default TSO performance group (1-255). Zero indicates no performance group was specified.
TSO_COMMAND	TSOCMDS	tsoCommand	8 characters	Command to be run during TSO/E logon
TSO_DEST	DFT-DEST	tsoDest	8 characters	Default SYSOUT destination
TSO_HOLDCLASS	DFT-SUBH	tsoHoldclass	1 character	Default hold class tsoSubmitclass DFTSUBM Default submit class
TSO_MSGCLASS	DFT-SUBM	tsoMsgclass	1 character	Default message class
TSO_SYSOUTCLASS	DFT-SOUT	tsoSysoutclass	1 character	Default SYSOUT class.

Table 1-3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Form	ACF2 Attribute	LDAP Attribute	Attribute Type	Description
TSO_SUBMITCLASS	DFT-SUBC		1 character	Default TSO submit class.
TSO_RBA	TSORBA	tsoRba	3 hexadecimal bytes	Revoke NA Value 'Y' if user is suspended or 'N' if the user is not suspended
TSO_ACCTPRIV	ACCTPRIV	tsoAcctPriv	bit field	Indicates user has TSO accounting privileges (for UADS updates with the TSO ACCOUNT command).
TSO_ALLCMDS	ALLCMDS	tsoAllCmds	bit field	Indicates the ability to bypass the CA ACF2 restricted command lists by entering a special prefix character.
TSO_MAIL	MAIL	tsoMail	bit field	Indicates that a user can receive mail messages from TSO at logon time.
TSO_JCL	JCL	tsoJcl	bit field	Indicates the ability to submit batch jobs from TSO and to use SUBMIT, STATUS, CANCEL, and OUTPUT commands (for example, use TSO SUBMIT).

Table 1-3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Form	ACF2 Attribute	LDAP Attribute	Attribute Type	Description
TSO_WTP	WTP	tsoWtp	bit field	Indicates that CA ACF2 displays write-to-programmer messages. CA ACF2 issues all violation and warning messages as WTPs. Specify this field for all TSO user logonid records so that they can receive CA ACF2 messages.
TSO_FSCRN	FSCRN	tsoFScrn	bit field	Indicates that a user can use the full-screen logon display.
TSO_MOUNT	MOUNT	tsoMount	bit field	Indicates permission to issue mounts for devices.
TSO_NOTICES	NOTICES	tsoNotices	bit field	Indicates a user can receive TSO notices at logon time.
TSO_OPERATOR	OPERATOR	tsoOperator	bit field	Indicates that a user has TSO operator privileges.
TSO_PROMPT	PROMPT	tsoPrompt	bit field	Indicates that CA ACF2 prompts a user for missing or incorrect parameters.
TSO_INTERCOM	INTERCOM	tsoIntercom	bit field	Indicates this user is willing to accept messages from other users through the TSO SEND command.
TSO_LGNACCT	LGN-ACCT	tsoLgnAcct	bit field	Indicates permission to specify an account number at logon time.

Table 1-3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Form	ACF2 Attribute	LDAP Attribute	Attribute Type	Description
TSO_LGNMSG	LGN-MSG	tsoLgnMsg	bit field	Indicates this user has permission to specify a message class at logon time.
TSO_LGNPERF	LGN-PERF	LGNPERF	bit field	Indicates permission to specify a performance group at logon time.
TSO_LGNPROC	LGN-PROC		bit field	Indicates permission to specify the TSO procedure name at logon time.
TSO_LGNRCVR	LGN-RCVR	tsoLgnRcvr	bit field	Indicates permission to use the recover option of the TSO or TSO/E Command Package. If not specified, the user cannot enter the PROFILE RECOVER command.
TSO_LGNFSIZE	LGN-SIZE	tsoLgnSoze	bit field	Indicates that this user is authorized to specify any region size at logon time (overriding TSOSIZE). A user can specify size at logon time without this field, but is restricted to a maximum size based on the TSOSIZE unless the LGN-SIZE field is in the logonid record.
TSO_LGNLTIME	LGN-TIME	tsoLgnTime	bit field	Indicates permission to specify the TSO session time limit at logon time.

Table 1-3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Form	ACF2 Attribute	LDAP Attribute	Attribute Type	Description
TSO_LGNUNIT	LGN-UNIT	tsoLgnUnit	bit field	Indicates permission to specify the TSO unit name at logon time.
TSO_TIME	TSOTIME	tsoTime	2-byte binary	Indicates a user's default TSO time parameter, which is the CPU time limit (in minutes) associated with the TSO session. The maximum value is 1440. Zero indicates no default TSO time parameter was specified.
ACCESS_CNT	ACC-CNT	accessCnt	READONLY	The count of the number of system accesses made by this logonid since it was created.
TSO_LGNDEST	LGN-DEST	tsoLgnDest	bit field	Indicates permission to specify a remote output destination at TSO logon that overrides the value specified in the DFT-DEST field.
TSO_CONSOLE	CONSOLE		bit field	Permits you to access the TSO/E CONSOLE facility.
ACCESS_DATE	ACC-DATE	accessDate	READONLY	ACCESS DATE
ACCESS_SRC	ACC-SRCE	accessSrc	READONLY	ACCESS SOURCE
ACCESS_TIME	ACC-TIME	accessTime	READONLY	ACCESS TIME
KERB_VIO	KERB-VIO	kerbVio	READONLY	PASSWORD KERB-VIO
KERB_CURV	KERBCURV	kerbCurv	READONLY	PASSWORD KERB-CURV
PASSWORD_DATE	PSWD-DAT	pswdDate	READONLY	PASSWORD DATE
PASSWORD_INV	PSWD-INV	pswdInv	READONLY	PASSWORD INTERVAL

Table 1-3 (Cont.) User Attributes for Target Resource Reconciliation and Provisioning

OIM Form	ACF2 Attribute	LDAP Attribute	Attribute Type	Description
PASSWORD_TOD	PSWD-TOD	pswdTod	READONLY	PASSWORD TIME OF DAY
PASSWORD_VIO	PSWD-VIO	pswdVio	READONLY	PASSWORD VIO
STAT_SECVIO	SEC-VIO	secVio	READONLY	STATISTICS
STAT_UPDTOD	UPD-TOD	updTod	READONLY	STATISTICS
CICS_ACF2CICS	ACF2CICS	cicsacf2cics	bit field	CICSACF2CICS
CICS_CL	CICSCL	cicscl	3 hexadecimal bytes	cicscl
CICS_ID	CICSID	cicsid	3 characters	CICS ID
CICS_IDLE	CICSIDLE	cicsidle	1-byte binary	cicsidle
CICS_OPT	CICSOPT	cicsopt	eight-characters	cicsopt
CICS_PRI	CICSPRI	cicspri	1-byte binary	cicspri
CICS_RSL	CICSRSL		3 hexadecimal bytes	Indicates CICS resource access key. For CICS support only.
MIN_DAYS	MINDAYS	minDays	1-byte binary	PASSWORD MIN DAYS
MAX_DAYS	MAXDAYS	maxDays	1-byte binary	PASSWORD MAX DAYS

Resource Rule Attributes for Target Resource Provisioning

[Table 1-4](#) lists resource rule attribute mappings between CA ACF2 and Oracle Identity Manager. The AssignUserToResourceRule and RemoveUserFromResourceRule adapters are used for resource rule provisioning operations.

Table 1-4 Resource Rule Attribute Mappings

Child Form Field	CA ACF2 Attribute	Description
RULE KEY	KEY	The high-level index of the data set name for which this rule is being written
TYPE	TYPE	The type of resource rule
ACCESS	ACCESS	System mode CA ACF2 should take when it validates access for this rule

Access Rule Attributes for Target Resource Provisioning

[Table 1-5](#) lists access rule attribute mappings between CA ACF2 and Oracle Identity Manager. The AssignUserToAccessRule and RemoveUserFromAccessRule adapters are used for access rule provisioning operations.

Table 1-5 Access Rule Attribute Mappings

Child Form Field	CA ACF2 Attribute	Description
DATASET ID	dsnmask	The name of the data set or a mask
RULE KEY	\$KEY	The high-level index of the data set name for which this rule is being written, or the VSM key of the rule set.
ACCESS READ	Read	Specifies read access and the action CA ACF2 should take when the environment matches
ACCESS WRITE	Write	Specifies write access and the action CA ACF2 should take when the environment matches
ACCESS EXECUTE	Execute	Specifies execute access and the action CA ACF2 should take when the environment matches
ACCESS ALLOCATE	Allocate	Specifies allocate access and the action CA ACF2 should take when the environment matches

Privilege Attribute for Target Resource Reconciliation and Provisioning

[Table 1-6](#) lists privilege attribute mapping between CA ACF2 and Oracle Identity Manager. MODIFYACF2USER adapter is used for privilege provisioning operations.

Table 1-6 Privilege Attribute Mapping

Child Form Field	CA ACF2 Attribute	Description
PRIVILEGE_NAME	privileges	Logong ID privileges

Reconciliation Rule

Reconciliation rules are used by the reconciliation engine to determine the identity to which Oracle Identity Manager must assign a newly discovered account on the target system.



See Also:

Oracle Fusion Middleware User's Guide for Oracle Identity Manager for generic information about reconciliation matching and action rules

During target resource reconciliation, Oracle Identity Manager tries to match each user profile fetched from CA ACF2 with existing CA ACF2 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 profile 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 profile against existing OIM Users. This is known as entity

matching. The same reconciliation rule is applied during this process. If an entity match is found, then a CA ACF2 resource is provisioned to the OIM User. Data for the newly provisioned resource is copied from the user.

The following is the reconciliation rule for target resource reconciliation:

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 ACF2.

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.

Reconciliation Action Rules

Reconciliation action rules specify actions that must be taken depending on whether or not matching CA ACF2 resources or OIM Users are found on Oracle Identity Manager when the reconciliation rule is applied.

[Table 1-7](#) lists the reconciliation action rules.

Table 1-7 Reconciliation Action Rules

Rule Condition	Action
No Matches Found	Assign to Administrator With Least Load
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. See *Oracle Fusion Middleware User's Guide for Oracle Identity Manager* for information about modifying or creating reconciliation action rules.

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 **OIMAcf2ResourceObject** 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.

Lookup Definitions Used for Provisioning and Reconciliation

These are the lookup definitions that are created when you install the connector or import the connector xml into Oracle Identity Manager.

Table 1-8 Lookup Definition and Descriptions

Lookup Definitions	Description
AtMap.ACF2	Used during attribute mapping for provisioning. Code Key is the ACF2 Process form attribute name. Decode Key is the corresponding LDAP Attribute.
ACF2.AccessLevels	Used while granting a user a resource rule for pre-population of values allowed for attributes.
ACF2.AccessMods	Used while granting user an access rule for pre-population of values allowed for attributes.
Lookup.AccessRuleNames	Contains the list of access rule keys reconciled using <code>ACF2 Find All Access Rules Task</code> . Used while granting user an access rule for pre-population of Access Rule Key.
Lookup.ResourceNames	Contains the list of resource rule keys reconciled using <code>ACF2 Find All Resource Rules Task</code> . Used while granting a user a resource rule for pre-population of Resource Rule Key.

2

Deploying the Agents of the CA ACF2 Connector on the Target System

Install the Pioneer Provisioning Agent and the Voyager Reconciliation Agent components of the CA ACF2 connector on the mainframe.

The following sections provide more information about installing, configuring, and using agents:

- [Deployment Requirements](#)
- [Installing the Mainframe Agents](#)
- [Configuring the Mainframe Agents](#)
- [Activating and Deactivating Reconciliation Exits](#)
- [Operator Interface for Mainframe Agents](#)
- [Uninstalling the Mainframe Agents](#)

Deployment Requirements

These are the deployment requirements for installing Pioneer and Voyager.

Before installing, refer the README that is contained in the connector installation media to learn about the new features, enhancements, and bug fixes. The following sections describe the installation and configuration of these agents:

Verifying Deployment Requirement

The following table lists the hardware, software, and authorization requirements for installing the Provisioning Agent - Pioneer and the Reconciliation Agent - Voyager.

Table 2-1 Deployment Requirements

Item	Requirement
Operating System	IBM z/OS 2.2, 2.3
Message Transport Layer	TCP/IP
ACF2 Identity Repository	Verify that the current PUT for z/OS is installed.
Target system user account for the Reconciliation and Pioneer Agents	ACF2-authorized user account with System Administrators privileges.
z/OS LE	Pioneer and Voyager are written using LE, and the System LE run options must be correct for proper execution.

Table 2-1 (Cont.) Deployment Requirements

Item	Requirement
Started Tasks	Both the Voyager and Pioneer Agents need a started task and a service account that has the privileges required to run the CA ACF2 system commands on the mainframe system. In addition, these agents function under a user account on the mainframe system. This user account must be created by the systems programmer before you deploy the agents.

 **Note:**

Both Voyager and Pioneer user accounts must be placed into the ACF2 database. These user accounts must have at least the permissions of the System Administrators group on the mainframe. These user accounts have permissions above those of ordinary administrators on the mainframe, which include Read, Write, Execute, and Modify privileges

Environmental Settings and Requirements

Ensure that the following requirements are met on the mainframe:

- Voyager and Pioneer each require approximately a 2-megabyte Region to work. Additionally, a subpool is created to contain Reconciliation changes for Voyager to access and send LDAP gateway. The subpool is in the ECSA and is generally small and is a temporary staging area for reconciliation requests. If there is an outage, Voyager saves the subpool to the //CACHESAV ddname specified in the Voyager STC, and when Voyager is restarted and the subpool is rebuilt, the CACHESAV file is reloaded into the subpool. Once the LDAP connects, the subpool data is sent to the LDAP.
- An ACF2 (LID) userid profile is required to start both Pioneer and Voyager. An ACF2 userid or LID for Pioneer requires special privileges. It acts as an ACF2 administrator with 'ACCOUNT and SECURITY' privileges.
- Voyager operates by using the following three standard ACF2 exits:
 - LIDPOST
 - NEWPXIT
 - EXPPXIT
- z/OS LE run options: ALL31 (ON) and STACK (131072,131072,ANYWHERE,KEEP,524288,524288). If the LE options are incorrect, it will result in a Pioneer or Voyager abend. Maintaining a specific password format is an example of the objective for which you use custom exits. CA ACF2 exits are engineered to be the last exits called in sequence, that allow existing exits to function normally. All of the exits used IDFACF2P(NEWPXIT), IDFACF2X(EXPPXIT), and IDFACF2E(LIDPOST) must be copied to an LPA Library, and then an IPL of z/OS is required to activate the exits. In addition, you require a module named "IDFCACHE" for all three exits to function

properly. It must also reside in the same LPA library as the exits. A 'SET PROG' member is then used to activate them.

 **Note:**

A system programmer must perform an IPL after a system component is changed or modified.

Installing the Mainframe Agents

The CA ACF2 Advanced connector is shipped with a pair of agents, one for provisioning and one for real-time reconciliation. If real-time reconciliation is not required, then install and start only the provisioning agent.

Before installation, review the [Deployment Requirements](#) section.

1. Extract the contents of the `ACF2-AGENTS-<TIMESTAMP>-<VERSION>.zip` file located in the connector installation media on to the computer hosting the mainframe.

The following files will be extracted:

- `CLISTLIB.XMIT`
- `JCLLIB.XMIT`
- `LINKLIB.XMIT`
- `PARMLIB.XMIT`
- `PROCLIB.XMIT`

2. Transmit the XMIT files extracted in the previous step to z/OS.

Use the following specifications during transmission:

- `RECFM=FB`
- `LRECL=80`
- `BLKSIZE=3120`
- `DSORG=PS`

For example, you may use 3270 or FTP to transfer the files.

The following datasets will exist on z/OS:

- `<HLQ>.CLISTLIB.XMIT`
- `<HLQ>.JCLLIB.XMIT`
- `<HLQ>.LINKLIB.XMIT`
- `<HLQ>.PARMLIB.XMIT`
- `<HLQ>.PROCLIB.XMIT`

 **Note:**

`<HLQ>` is the high-level-qualifier used when transmitting the files to z/OS.

- For each of the files transmitted in the previous step, execute the following command at the TSO prompt: `TSO RECEIVE INDA('<HLQ>.<FILE>.XMIT')`. When prompted to specify restore parameters, enter `DA('<HLQ>.<FILE>')`.

For example, if the high-level qualifier is `IDF` and the file is `CLISTLIB.XMIT`, execute the following command: `TSO RECEIVE INDA('IDF.CLISTLIB.XMIT')`, and when prompted, respond with: `DA('IDF.CLISTLIB')`.

The following datasets will exist on z/OS:

- `<HLQ>.CLISTLIB`
- `<HLQ>.JCLLIB`
- `<HLQ>.LINKLIB`
- `<HLQ>.PARMLIB`
- `<HLQ>.PROCLIB`

 **Note:**

In the preceding datasets, replace `<HLQ>` with the high-level-qualifier used when receiving the previously transmitted files.

- Edit each of the following installed job streams and provide values for any placeholders in them.

- `<HLQ>.CLISTLIB.ENVINFO`
- `<HLQ>.JCLLIB.CREATDSN`
- `<HLQ>.JCLLIB.CRTLOGDN`
- `<HLQ>.JCLLIB.IEBCOPYL`
- `<HLQ>.JCLLIB.IEBCOPYP`
- `<HLQ>.JCLLIB.IEBCPYPR`
- `<HLQ>.JCLLIB.KEYMODR`
- `<HLQ>.PARMLIB.PROGID`
- `<HLQ>.PROCLIB.PIONEER`
- `<HLQ>.PROCLIB.STARTUP`
- `<HLQ>.PROCLIB.VOYAGER`
- `<HLQ>.PROCLIB.WRAPUP`
- `<HLQ>.JCLLIB.LOADDSN1`

 **Note:**

Replace `<HLQ>` with the high-level-qualifier used when receiving the previously transmitted files.

The following table lists the installation placeholders, their description, and example.

Table 2-2 Installation Placeholders

Placeholder	Description	Example
++hlq++	The high-level qualifier where the product is to be installed. If there are multiple segments, all should be included.	IDF
++vol++	The volume where the product is to be installed.	SDWRK1
++lpalib++	The DSN of the data set that contains customized lpalibs. Customize based on z/OS environment.	USER.LPALIB
++parmdtr++	The name of the PARMLIB XMIT that was transmitted to z/OS (without the .XMIT).	<HLQ>.PARMLIB
++parmlib++	The DSN of the data set that contains customized parmlibs. Customize based on z/OS environment.	USER.PARMLIB
++procdtr++	The name of the PROCLIB XMIT that was transmitted to z/OS (without the .XMIT).	<HLQ>.PROCLIB
++proclib++	The DSN of the data set that contains customized proclibs. Customize based on z/OS environment.	USER.PROCLIB
++linkdtr++	The name of the LINKLIB XMIT that was transmitted to z/OS (without the .XMIT).	<HLQ>.LINKLIB
++linklib++	The DSN where the LINKLIB XMIT that was received.	<HLQ>.LINKLIB
++rexxdtr++	The name of the CLISTLIB XMIT that was transmitted to z/OS (without the .XMIT).	<HLQ>.CLISTLIB
++rexxlib++	The DSN where the CLISTLIB XMIT that was received.	<HLQ>.CLISTLIB
++pionprms++	The DSN of the control (configuration) file for the provisioning agent.	PIONEER.CONTROL.FILE
++voyprms++	The DSN of the control (configuration) file for the reconciliation agent.	VOYAGER.CONTROL.FILE

 **Note:**

Replace <HLQ> with the high-level-qualifier used when receiving the previously transmitted files.

For example, in the following snippet from `CREATEDSN`, replace the placeholders `+hlq++` and `++vol++` with values such as `IDF` and `SDWRK1`:

```
//*
//S1      SET   PHLQ=++hlq++.PIONEER
//S2      SET   VHLQ=++hlq++.VOYAGER
//S3      SET   PVOL=++vol++
//S4      SET   VVOL=++vol++
//*
```

The following snippet displays the placeholders replaced with values:

```
//*
//S1      SET   PHLQ=IDF.PIONEER
//S2      SET   VHLQ=IDF.VOYAGER
//S3      SET   PVOL=SDWRK1
//S4      SET   VVOL=SDWRK1
//*
```

- Execute each of the following job streams in the order as shown in the following table to complete installation.

Table 2-3 Job Streams to Execute

Job Stream	Description
<HLQ>.JCLLIB.IEBCOPYP	Copies PARMLIB members to user PARMLIB.
<HLQ>.JCLLIB.IEBCPYPR	Copies PROCLIB members to user PROCLIB.
<HLQ>.JCLLIB.IEBCOPYL	Copies exit routines to use LPA library.
<HLQ>.JCLLIB.CREATDSN	Allocates run time data sets, deleting the data sets first if they already exist.
<HLQ>.JCLLIB.LOADDSN1	Copies PIONEER & VOYAGER configuration (control) files.
<HLQ>.JCLLIB.ACF2DEL	Deletes pre-existing users and data sets that are overwritten by the installation.
<HLQ>.JCLLIB.ACF2DEF	Defines users and permissions required to run the mainframe agent STCs.

 **Note:**

In the above, replace `<HLQ>` with the high-level-qualifier used when receiving the previously transmitted files.

The installation of the provisioning and reconciliation agents is complete. At this point, you can optionally remove the XMIT datasets that were originally transmitted to z/OS.

Configuring the Mainframe Agents

After installing Pioneer and Voyager, you must configure the mainframe agents to receive requests from the gateway and to also send responses to the gateway.

This section discusses the following topics:

- [Configuring the Provisioning Agent](#)
- [Configuring the Reconciliation Agent](#)

Configuring the Provisioning Agent

You must configure the provisioning agent to receive requests from the LDAP gateway (which comes from OIM).

Edit the `<HLQ>.PIONEER.CONTROL.FILE` file to configure the behavior of the provisioning agent. `<HLQ>` is the high-level-qualifier that is specified when you install the agents. See [Installing the Mainframe Agents](#) for more information.

Table 2-4 Provisioning Agent Parameters

Parameter	Value	Description
TCPN	TCPIP	The name of the TCP/IP STC where the agent is executing.
IPAD	0.0.0.0	Do not change.
PORT	9999	The TCP/IP port that the agent will listen on.
CRLF	Y or N	Must be set to Y for version 6+ of the LDAP Gateway. Set to N for version 5.
DEBUG	Y or N	Y turns on debugging and output goes to //DEBUGOUT. Beware as DEBUG=Y produces a lot of output and is not recommended unless instructed by technical personnel.
ESIZE	16	This is the only valid value. This parameter is for the AES128 encryption and decryption.
POST_PROC_ALIAS	T or F	If T, all LDAP Alias requests are processed. If F, all LDAP Alias requests are rejected.
IDLEMSG	Y or N	If set to Y, an idle message displays every hour. if set to N, idle messages are not displayed on the log.
DEBUGOUT	SYSOUT, CLASS (X)	X should be a single character, valid JES2 class. Used when DEBUG=Y is specified.

Table 2-4 (Cont.) Provisioning Agent Parameters

Parameter	Value	Description
SPIN_CLASS	X	X should be a single character, valid JES2 class. Used when <code>DEBUG=Y</code> is changed to <code>DEBUG=Y</code> via the <code>modify</code> command.
AUDIT	AUDIT=YES, SYSOUT, CLASS (X) when audit logs are needed or NO	If set to YES, records are sent to <code>//AUDTLOG</code> . If set to NO, <code>//AUDTLOG</code> is not generated and no audit logs are recorded.
FILTER	YES or NO	If set to NO, no filtering of inbound LDAP requests is performed. If set to YES, the F1 and F2 parameters are examined for filter criteria.
F1	Up to 8 comma-separated values	ACF2 INSERTS and CHANGES are examined for these values. The supported values are the standard ACF2 attributes for the LID. For example, SECURITY, AUDIT, READALL. If request containing values specified in F1 are encountered, PIONEER rejects those requests.
F2	See F1	See F1

Configuring the Reconciliation Agent

You must configure the reconciliation agent to send incremental responses to the gateway.

Edit the `<HLQ>.VOYAGER.CONTROL.FILE` file to configure the behavior of the reconciliation agent. `<HLQ>` is the high-level-qualifier specified when installing the agents. See [Installing the Mainframe Agents](#) for more information.

Table 2-5 Reconciliation Agent Parameters

Parameter	Value	Description
SUBPOOL_SIZE	0200K to 7500K	Subpool size desired for storage of reconciliation messages captured from exits. This storage is allocated above the 16M line.
TCPN	TCPIP	The name of the TCP/IP STC where the agent is executing.
IPAD	999.999.999.999 or ldap.example.com	LDAP destination IP address or hostname (up to 40 characters).
PORT	9999	LDAP destination port that is listening to the incoming agent messages.

Table 2-5 (Cont.) Reconciliation Agent Parameters

Parameter	Value	Description
CRLF	Y or N	Must be set to Y for version 6+ of the LDAP Gateway . Set to N for version 5.
DEBUG	Y or N	Y turns on debugging and output goes to //DEBUGOUT. Beware as DEBUG=Y produces a lot of output and is not recommended unless instructed by technical personnel.
ESIZE	16	This is the only valid value. This parameter is for the AES128 encryption and decryption.
CACHE_DELAY	0 to 999	This is 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, otherwise the code is 0.
POST_PROC_ALIAS	T or F	If T, all LDAP Alias requests are processed. If F, all LDAP Alias requests are rejected.
IDLEMSG	Y or N	If set to Y, an idle message displays every hour. If set to N, no idle messages are logged.
DEBUGOUT	SYSOUT, CLASS (X)	X should be a single character, valid JES2 class. Used when DEBUG=Y is specified.
AUDIT	YES or NO	Records output to //AUDTLOG if set to YES.
VOYAGER_ID	YES or NO	This value will be included in the LDAP logs for diagnostics.
FILTER1	YES or NO	Filter reconciliation messages based on the criteria provided. See Understanding the Reconciliation Agent FILTER Parameter .
FILTER2	See FILTER1	See FILTER1.

Understanding the Reconciliation Agent FILTER Parameter

You can configure Voyager to filter responses that are sent to the LDAP gateway.

Voyager has the ability to FILTER command output to the LDAP. The processing sequence is as follows:

```
FILTER1=YES,A=PREFIX,V=TEST,TEST10
```



Note:

The values of A= and V= must be less than 10 characters.

When the value of FILTER parameter is set to YES in Voyager, then the following sequence occurs:

1. Voyager polls the cache area.
2. Performs a LIST xxxxx (LID) from the subpool.
3. Verifies that the filter=yes.
4. Scans for the values.
 - If the values match the stored control file values, then the subpool message is not passed to the LDAP.
 - If the value does not match the stored control file values, then the subpool message is passed to the LDAP and is removed.

Activating and Deactivating Reconciliation Exits

You must activate system exits for capturing and reacting to changes in the security system in order to make use of real-time reconciliation and the reconciliation agent.

- [Activating Reconciliation Exits](#)
- [Deactivating Reconciliation Exits](#)

Activating Reconciliation Exits

Activate the system exits to capture security system changes in real-time.

To do so, run the following command from the z/OS operator interface:

```
T PROG=78
```

Deactivating Reconciliation Exits

Deactivate the system exits to disable the reconciliation of real-time changes to the security system.

To do so, run the following command from the z/OS operator interface:

```
T PROG=79
```

Operator Interface for Mainframe Agents

Both provisioning and reconciliation agents have an operator interface, and you can control the agents by passing commands through the interface.

The following topics are discussed in this section:

- [Provisioning Agent Commands](#)
- [About Reconciliation Agent Commands](#)

Provisioning Agent Commands

Pass the Pioneer provisioning agent commands through the operator interface to control Pioneer.

Table 2-6 Provisioning Agent Commands

Command	Description
T PROG=ID	APF authorizes <HLQ>.LINKLIB - required to start the agent.
S PIONEER	Starts the agent.
F PIONEER, SHUTDOWN	Shuts down the agent.
F PIONEER, STATUS	Sends a status request to the agent.
F PIONEER, DEBUG=Y	Enables debug-level (detailed) log output.
F PIONEER, DEBUG=N	Disables debug-level (detailed) log output.

 **Note:**

This interface through the z/OS modify command is a *single-threaded* system. Commands are queued and may take a few seconds before the agent acknowledges them.

About Reconciliation Agent Commands

Pass the Voyager reconciliation agent through the operator interface to control Voyager.

[Table 2-7](#) Voyager reconciliation agent commands and their descriptions.

Table 2-7 Reconciliation Agent Commands

Command	Description
T PROG=ID	APF authorizes <HLQ>.LINKLIB - required to start the agent.
T PROG=78	Activates system exits - required for real-time reconciliation. See Activating and Deactivating Reconciliation Exits .
S VOYAGER	Starts the agent.
F VOYAGER, SHUTDOWN	Shuts down the agent.
F PIONEER, STATUS	Sends a status request to the agent.
F PIONEER, DEBUG=Y	Enables debug-level (detailed) log output.
F PIONEER, DEBUG=N	Disables debug-level (detailed) log output.
S STARTUP	Creates subpool231 and inserts the IDF Token in storage for storing reconciliation events. This is optional as the same functionality is executed when Voyager is started. See the following note for permissions required to execute STARTUP.

Table 2-7 (Cont.) Reconciliation Agent Commands

Command	Description
S WRAPUP	Deletes the IDF token and subpool 231 created in storage. This is optional as same functionality is executed when Voyager is shutdown, but can be executed if required explicitly. See the following note for permissions required to execute WRAPUP.

 **Note:**

- The interface through the z/OS modify command is a *single-threaded* system. Commands are queued and take a few seconds before the agent acknowledges them.
- <HLQ> is the high-level-qualifier specified when installing the agents.
- For STARTUP and WRAPUP commands to execute successfully, provide access to ACF2 default STC ID at site on dataset high level qualifier <HLQ> specified while installing the agents.

The following are example commands assuming default STC ID as ACFSTCID

```
ACF
SET RULE
RECKEY <HLQ> ADD (- UID (*****ACFSTCID) READ (A)
WRITE (A) EXEC (A) )
F ACF2,RELOAD(<HLQ>)
END
```

Here, ACFSTCID is the LID in UID string. Update UID string as per ACFFDR at you site.

Uninstalling the Mainframe Agents

Uninstalling removes the provisioning and reconciliation agents from the ACF2 connector.

To uninstall Pioneer and Voyager, do the following:

1. Shut down Pioneer and Voyager.
2. Execute wrapup (/s wrapup) to ensure subpool231 and IDF token are cleared from storage.
3. Edit and Run ACF2DEL to delete permissions and requests.
4. Run Prog79 using /T prog=79 to disable Exits.
5. Remove APF Authorization to the load library using APF DELETE DSNAME (loadlib) VOLUME (name). This can be achieved by replacing ADD with DELETE in

the PROGID member for the corresponding PARMLIB and executing the member through /T PROG=ID from operator console.

6. Delete XMITs and the corresponding received datasets (LINKLIB,CLISTLIB,JCLLIB,PROCLIB and PARMLIB).

3

Installing and Configuring the LDAP Gateway

You can install the LDAP gateway on Windows and Linux platforms.

The following topics describe the system requirements, LDAP gateway concepts, and procedures to install and configure the LDAP gateway:

- [System Requirements](#)
- [LDAP Gateway Concepts](#)
- [Files and Directories that Comprise the LDAP Gateway](#)
- [Installing the LDAP Gateway](#)
- [Configuring the LDAP Gateway](#)
- [Configuring Windows Service](#)
- [Starting the LDAP Gateway](#)

System Requirements

These are the recommended system requirements that are designed to give you optimal system performance from the LDAP gateway.

However, individual performance may vary depending on actual system components in use and the number of objects being managed on the target system.

The following are the minimum system requirements:

- Windows Server (2012) and Linux (RHEL)
- 2 GHz Single-Core Processor
- 4 GB RAM
- 10 GB Hard disc drive
- 1 Network Interface

The following are the recommended system requirements:

- Windows Server (2012) or Linux (RHEL)
- 2 GHz Multi-Core Processor
- 16 GB RAM
- 50 GB Hard disc drive
- 1 Network Interface

The following are the prerequisites required to install the LDAP Gateway:

- 64-bit Linux or Windows Server 2016 or later.
- The LDAP Gateway requires Oracle Java JRE 1.7, 1.8, or 1.10.
- A software license file (`license.lic`) available in the connector installation media.

If you do not have Java, the installer will redirect you to the Oracle website to install Java. Re-run the LDAP Gateway installer once Java is installed.

LDAP Gateway Concepts

This section discusses the following optional features of the LDAP Gateway:

- [About Encrypting Data](#)
- [About Caching Layer](#)
- [About Scheduled Recon Utility](#)
- [About Parsing Grammar Protocol 1.0](#)

About Encrypting Data

An `encryption.properties` file exists in the `conf/` directory. This file allows the ability to configure what properties associated with connectors should be managed as encrypted values.

For example,

```
file.customer-configuration=adminUserPassword,altAdminUserPassword
```

This example defines that there exists a properties file called `customer-configuration.properties` that contains the sensitive properties `adminUserPassword` and `altAdminPassword`. This definition is consumed when the gateway first starts up. If the property file exists on the disk, the gateway searches for that property file and replaces any cleartext values in those properties with an encrypted version.

It is similar to connector definitions. For example, for the CA ACF2 connector, `class.ACF2Module=_SecretKeyValue_` defines that there exists a connector called `ACF2Module` whose associated property files contain the sensitive property of `_SecretKeyValue_` that needs to be secured by the gateway.

When the gateway starts, it uses the `encryption.properties` file to examine the properties that need to be represented in their encrypted format. Encrypted values within property fields are always represented using the format - `ENC(<ENCRYPTED STRING>)`. To add or replace an existing encrypted value with a new value, replace the entire encryption string if present (including the `ENC()`) with a new clear text value, and then restart the gateway. Once the gateway restarts, the newly added clear text value goes through an encryption process with the result being written back out to the property file replacing the original clear text value.

During the encryption process, the encryption framework used by the gateway automatically detects the highest level of encryption possible by examining the version of the Java Virtual Machine running along with any additional encryption libraries that may have been installed alongside the JVM. By default, Java 1.8 support 128-bit AES encryption and Java 1.7 support 40-bit AES encryption. Additional encryption libraries by BouncyCastle can be installed into the JVM allowing for up to 256-bit AES encryption.

The encryption process in the gateway also allows for automatic migration of encryption values from a lower bit strength to a higher strength as it becomes

available. For example, if the gateway is initially deployed on a system running Java 1.7 with 40-bit AES and that system is upgraded to Java 1.8 running 128-bit AES, then upon the next restart of the gateway, all encrypted values remaining at the 40-bit AES level are automatically re-encrypted at the higher 128-bit and stored back out in the property files. This process eliminates the need to manually replace the values in every property file in order to take advantage of the higher bit strength.

The private key located in the `idf.properties` file is used for all the encryption and decryption performed by the gateway. It is recommended that access should be restricted to this file.

 **Note:**

Once the gateway is deployed and started up for the first time, the value of the autogenerated encryption key in the `idf.properties` file should not be changed. However, the file name and its location can be easily changed. For example, to store the `idf.properties` file to a more secure location, the default location (where the gateway resides) can be overridden and defined as `system.idfprops.filepath=<absolute path of the new file>` in the `customer-configuration.properties` file.

About Caching Layer

A Caching layer is a temporary storage area where frequently accessed data is stored for rapid access.

The IDF LDAP Gateway features an optional and configurable caching layer.

An expiration policy defines the time dependency for the cached resource. For example, the `cachingMaxAge` parameter specifies the maximum time in minutes when the data is not in sync with the target systems. You can pair the caching layer with a real-time reconciliation or with a scheduled reconciliation to maintain the most recently updated data in the caching layer. This improves the performance of the LDAP Gateway. The caching layer also opens the LDAP Gateway up to more advanced features defined by the LDAPv3 RFC.

The caching layer, when enabled, offers the following benefits:

- Faster search operations (when the cache is primed)
- A unified Base DN for both provisioning and reconciliation data

When paired with the Embedded DS (default behavior), the caching layer offers these additional benefits:

- The ability to perform advanced LDAP search filters against the Gateway
- The ability to query an RFC compliant ChangeLog for delta reconciliation

 **Note:**

In an environment where the items noted above may not be required, the caching layer can be turned off entirely by setting the `cnctr.coreBean.nexus.cachingEnabled=false` in the `customer-configuration.properties`.

The LDAP Gateway can suffer a performance penalty when all of the following conditions are met:

- There is no data in the cache, or the cache is stale based on configuration
- An LDAP search operation is performed to retrieve the children of an Organizational Unit - e.g. the contents of `ou=People`
- The target Adapter only returns *key* information when returning a list of objects.

Performing an LDAP search operation against such adapters to retrieve the children of an Organization Unit returns only DN's (along with RDN components).

- The `cachingIterateBehavior` property remains set to the default of `AUTO` and not overwritten within the `customer-configuration.properties` file.

In this case, an LDAP search operation initially retrieves the list of results, containing only DN and RDN values. The LDAP Gateway caching layer then iterates through each result, fetching and caching the details from the target Adapter. Finally, the full set of results will be returned to the LDAP client.

To avoid this scenario, it is recommended that you use the caching layer in combination with Scheduled Recon or Real-time recon. With reconciliation setup and the staleness settings configured properly the above conditions will not be met.

**Note:**

See [About Scheduled Recon Utility](#).

About Scheduled Recon Utility

Scheduled Reconciliation allows for establishing a periodic synchronization between the Identity Store associated with the LDAP Gateway and that is represented by a target system reachable by way of a connector.

The Scheduled Recon Utility (provided by `dist/scheduled-recon.jar`) is a tool that ships with the IdentityForge LDAP Gateway. It provides the ability to perform a full recon against a configurable target system, placing the results in the Gateway's internal identity store.

- For connectors that already support reconciliation against the Internal identity store such as ACF2.
- For connectors that do not support reconciliation, the connectors rely solely on the Scheduled Recon Utility for both scheduling and providing the capabilities necessary to simulate a traditional batch recon process.

An example properties file that defines the reconciliation setup and behavior - `scheduledrecon.properties.example` - is provided in the `conf/` folder.

Configuration

An example properties file, `scheduled-recon.properties.example` file that defines the reconciliation setup and behavior is available at (`.../IDFLDAPGateway-6/conf/...` folder). Use this file to configure the scheduled recon. Create a `scheduled-recon.properties` file in the `conf` folder and copy all the settings from the `scheduled-`

recon.properties.example file. A scheduled-recon.properties file containing the configuration details for the recon operation can be provided via the -h argument.

```
D:\ldapgateway6.0-v6.0.0-rc1\bin> run-recon.bat -h
Usage: GatewayBatchRecon [-h] [-l <loglevel>] -p <properties file path>
-h                               : Help
-loglevel <level>                : Define logging level. Possible values are 'severe','warning','info','fine','finer','finest'
(Default is 'warning')
-logfile <filepath>              : Path to log file
-p <properties filepath>         : Path to file that contains the property definitions that drive this application
```

A batch file called run-recon.bat located in the “bin” folder can be used to start the scheduled recon utility. The basic command structure for executing this batch file is as follows:

```
...\\ldapgateway6\bin>run-recon.bat -l "warning" <location of the log file> -p
"D:\ldapgateway6\conf\scheduled-recon.properties".
```

```
D:\ldapgateway6.0-v6.0.0-rc1\bin> run-recon.bat -l "warning" -p "D:\ldapgateway6.0-v6.0.0-rc1\conf\scheduled-recon.properties"
May 25, 2017 2:19:38 PM com.identityforge.tools.recon.Configurations load
INFO: Attempting to load following properties file: D:\ldapgateway6.0-v6.0.0-rc1\conf\scheduled-recon.properties
May 25, 2017 2:19:40 PM com.identityforge.tools.recon.Main main
```

Execute the run-recon.bat with a minimum set of arguments passed in. For example,

```
D:\ldapgateway6.0-v6.0.0-rc1\bin>run-recon.bat -l "Debug" -p "D:\ldapgateway6.0-v6.0.0-rc1\conf\scheduled-recon.properties"
May 22, 2017 4:22:39 PM com.identityforge.tools.recon.Configurations load
INFO: Attempting to load following properties file: D:\ldapgateway6.0-v6.0.0-rc1\conf\scheduled-recon.properties
May 22, 2017 4:22:42 PM com.identityforge.tools.recon.Reconciliation getMetaIdMap
INFO: Number of seconds to retrieve list of uids from Meta Directory: 0s
May 22, 2017 4:22:42 PM com.identityforge.tools.recon.Reconciliation getTargetUids
INFO: Number of seconds to retrieve list of uids from target system: 0s
May 22, 2017 4:24:33 PM com.identityforge.tools.recon.Reconciliation performReconciliation
INFO: Number of seconds to retrieve, analyze and store the details for 31 objects: 111s
May 22, 2017 4:24:33 PM com.identityforge.tools.recon.Reconciliation performReconciliation
INFO: totals: Added=1 Updated=1 Deleted=0
May 22, 2017 4:24:33 PM com.identityforge.tools.recon.Main main
INFO: Exiting GatewayBatchRecon
Press any key to continue
```

About Parsing Grammar Protocol 1.0

Grammar is necessary for properly parsing user and group listings that come into the gateway from the mainframe agent during search requests and reconciliation events.

The grammar represents line-by-line parsing instructions that convert the semi-structured textual data into LDAP attributes and their respective values. Each line (ending in CRLF) of the listing received from the agent can be represented by an individual grammar definition and specified in the grammar file. The grammar file is present in the <conf/parser-grammar/> folder.

For example, following is the ACF2 user listing:

```
PIONEER                                PIONEER          VPIONEER-STC
CLIENT() COMPANY() DEPT() GRP() LEVEL() LOCATION()
PROFILE() REGION() SBCLIENT()
PRIVILEGES                             ACCOUNT SECURITY STC
ACCESS                                 ACC-CNT(0) ACC-DATE(00/00/00) ACC-TIME(00:00)
PASSWORD                               KERB-VIO(0) KERBCURV() PSWA1TOD(00/00/00-00:00)
PSWD-DAT(00/00/00) PSWD-INV(0) PSWD-TOD(00/00/00-00:00)
PSWD-VIO(0) PSWDCVIO(0) PWP-DATE(00/00/00) PWP-VIO(0)
TPXPROF()
TSO                                    DFT-PFX(PIONEER)
STATISTICS                             CRE-TOD(05/17/18-00:13) SEC-VIO(0)
UPD-TOD(05/17/18-00:13)
RESTRICTIONS                           PREFIX(PIONEER) UXHOLD5()
```

Using the above listing, if you want to parse out the KERB-VIO value from the listing and assign it to an LDAP attribute called "kerbvio", the following <Line> element can be constructed in the grammar file.

```
<Line id="kerbvioVal" enabled="yes" sig="[ ]*KERB-VIO = (?
&lt;kerbvio&gt;.*)" />
```

The signature attribute (sig) in the Line element above is a regex that represents the rules for pulling out the value and assigning it to an LDAP attribute. Regex named groups are used as the convention for assigning the discovered values to LDAP attributes exposed through the connector.

The following table lists the attributes of a line element. The allowed values for these attributes are **yes** or **no**.

String	Definition
id	Unique ID that is given to the Line definition. Used primarily for internal referencing purposes, such as with the 'dependson' attribute Values Allowed: [any] Behavior: Required
enabled	Specifies whether the Line is eligible for participating in the Parsing process. This flag is used mainly to allow the customers to override files (turn off lines). Behavior: Optional Defaults to: yes
signature	Defines the rules for what values are to be extracted for each line of the listing and which LDAP attribute(s) should be assigned the values. Behavior: Required
required	Defines if an attribute is required or not. Default to: yes
multiline_sig	An optional regex expression to define the signature of a follow-on line that could represent whether the value was wrapped around two additional lines in the document Values Allowed: [any valid regex containing attribute matching key and attribute name]. Behavior: Optional Defaults to: empty value
repeats	Represents whether the line can show up multiple times in the document. If set to "no", once the line is found, this Line definition is not evaluated again for the rest of the document. Behavior: Optional Defaults to: No
overflow	Represents whether data for an associated attribute can overflow to next line. In case of an overflow, the final value of an attribute will be derived by concatenating all values. Behavior: Optional Defaults to: No

String	Definition
<code>multivalue_parser</code>	An optional regex expression that defines how the found values are to be parsed out and turned into a multivalued list, such as using <code>'(\S+)'</code> to parse values that are space delimited. Values Allowed: [any valid regex] Behavior: Optional Defaults to: empty value
<code>applyCompositeRef</code>	An optional comma separated list of composite attributes to be built immediately after processing the line. Each value in the comma separated list should correspond to the "id" attribute of a CompositeAttribute definition.
<code>defaultvalue</code>	Defines the default value for an attribute. If this line does not match with any line of input, then this default value will be assigned to attribute. Behavior: Optional

Customizing Grammar Rules

The grammar file with the default grammar is present in the `conf` folder. It parses user and group listings that come into the gateway from the mainframe agent during search requests and reconciliation events. You can apply new grammar rules to append to or override rules that come out of the box. To define new grammar rules or override the existing rules, create a grammar file `parser-grammars.cust` file in the `<conf/parser-grammar/ >` folder.

Note:

- If the Id of the existing attribute matches with the attribute in the grammar line, it overrides the existing grammar definition.
- If the Id of the existing attribute does not match with the attribute in the grammar line, it creates a new grammar definition.

Key Considerations

- The `parser-grammars.cust` grammar file must be at the same location where the `parser-grammars` file.
- The name of the grammar file must be the same except the `cust` extension.
- For the grammar definitions to override, the ID attribute from both the files should match.

Nomenclature of the parsing grammar files

Each grammar file is named for the type of operation and listing it is responsible for parsing.

For example, for ACF2:

For user extraction use the following:

- `acf2_FindAllUsers.xml` – fetches the IDs of all users.
- `acf2_FindUserById.xml` – fetches all the details of a single user (for the given ID).

Overriding default existing grammar definitions

The grammar definitions specified in the grammar file `parser-grammars.cust` override the default grammar definitions specified in the property files. To enable overriding of the particular line, the ID attribute in the custom provided attribute should match with the default grammar definition.

For example, if the default grammar definition in the property file and the definition specified in the custom grammar file is as shown in the following lines, then the definition is disabled and the line is not parsed.

```
<Protocol><Lines>
<Line id="elId" enabled="yes" sig="[ ]*ELID[ ]*=[ ]*(?<ELID>.*)" />
</Lines>/Lines>
```

```
<Protocol><Lines>
<Line id="elId" enabled="no" sig="[ ]*ELID[ ]*=[ ]*(?<ELID>.*)" />
</Lines></Protocol>
```

New grammar definitions

New grammar definitions can be specified in the grammar file `parser-grammars.cust`. For example, the following grammar definition is used to get values of `DEPT_ACID=001` `DEPT_NAME=hr`.

```
<Protocol><Lines>
="deptAcid" enabled="yes" sig="[ ]*DEPT_ACID[ ]*=[ ]*(?
<deptacid>.*?)
[ ]*DEPT_NAME[ ]*=[ ]*(?<department>.*)" />
</Lines></Protocol>
```

Files and Directories that Comprise the LDAP Gateway

These are the files and directories that comprise the LDAP Gateway.

Table 3-1 Files and Directories that Comprise the Gateway

Files and Directories	Description
bin	The <code>bin/</code> folder contains run scripts for the components of the LDAP Gateway: <ul style="list-style-type: none">• <code>run.bat (.sh)</code> - Used to start the Gateway server• <code>stop.sh</code> - Used to stop the Gateway when run with <code>nohup</code>• <code>run-migration.bat (.sh)</code> - Used to migrate between versions of the product• <code>run-recon.bat (.sh)</code> - Used to run the scheduled recon utility. See About Scheduled Recon Utility.• <code>stop-recon.sh</code> - Used to stop the Scheduled Recon Utility when run with <code>nohup</code>• <code>install-license.bat (.sh)</code> - Used to install a <code>license.lic</code> file found in the <code>conf/</code> folder
conf	The <code>conf/</code> folder contains the files required to configure a connector. For example, <ul style="list-style-type: none">• <code><connector>.properties</code> - Contains connector-specific configuration• <code>customer-configuration.properties</code> - Contains the LDAP Gateway configuration
dist	The <code>dist/</code> folder contains the distributable JAR files. For example: <ul style="list-style-type: none">• <code>idfserver.jar</code> - LDAP Gateway server• <code>migration-utility.jar</code> - Utility for migrating between product versions• <code>scheduled-recon.jar</code> - Represents the scheduled recon utility. See About Scheduled Recon Utility.• <code>property-validator.jar</code> - Used to validate (lint) <code>.properties</code> files
dsroot	The <code>dsroot/</code> folder contains configuration files and data related to our Embedded DS persistence layer.
logs	The <code>logs/</code> folder contains all the audit logs of the transactions.
schema	The <code>schema/</code> folder contains files that determine the attributes types supported by the LDAP Gateway.

Installing the LDAP Gateway

Install the LDAP Gateway on Windows and Linux platforms.

Note:

During installation of the LDAP Gateway, if a previous installation is detected, you can either upgrade or continue with the fresh installation. If you plan to upgrade, ensure to perform the following preupgrade steps:

- Stop the running instance of the Gateway. If you are using Windows Service to run the Gateway, then uninstall the Windows Service.
- Shut down any Agent (for example, Pioneer or Voyager) running on the target environment.
- Disable any cron jobs.

See [System Requirements](#) to ensure that the target machine has the suitable specifications.

To install the LDAP Gateway, do the following:

1. To display the **LDAP Gateway Setup Wizard**, do the following:

Note:

The IDFLDAPGateway-6-linux-64-installer.run and IDFLDAPGateway-6-windows-64-installer.exe files are available in the IDF_LDAP_GATEWAY_VERSION.zip located in the connector installation media.

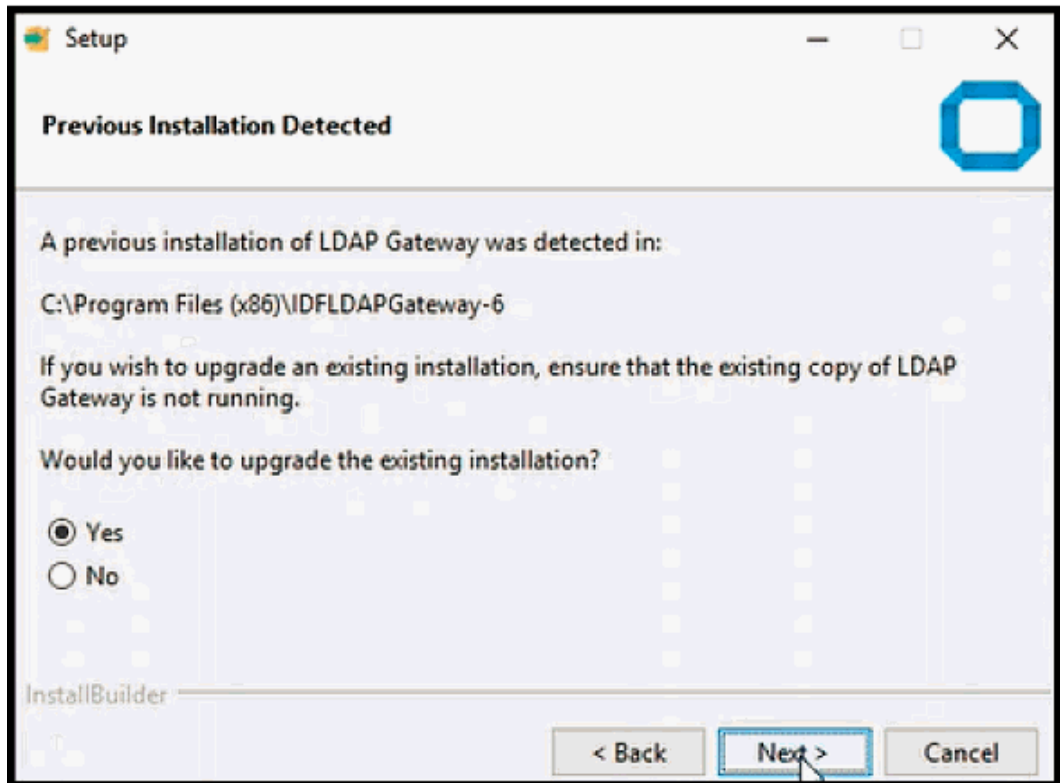
- If you are using a Linux operating system, then run the IDFLDAPGateway-6-linux-64-installer.run file.
- If you are using a Microsoft Windows operating system, then run the IDFLDAPGateway-6-windows-64-installer.exe file.

The **LDAP Gateway Setup Wizard** is displayed.

2. Click **Forward** to proceed.

The EULA is displayed.

3. Accept the **EULA**, and then click **Next** to proceed.
4. If an instance of LDAP Gateway is already installed, then that installation is detected as shown in the following image.



5. If you want to upgrade, click **Yes** and then click **Next** to proceed. If you click **No**, then fresh installation will continue.

 **Note:**

To upgrade from version 5.x to 6.x, you need to provide the location of the existing installation folder location and the path of the valid license file. If the install folder location is same, then the installer detects and creates a backup of the entire folder of the previous version with a suffix pre- and a timestamp. This can be verified at the install location. The backup of the entire folder happens only once when you are upgrading from v5 to v6. For example, if you already have a Gateway version 5.3 installed on your system, and you want to install Gateway version 6, a backup folder for the files of 5.3 is created at the install location.

The **Ready to Install** window is displayed. Continue from Step 7.

6. If no instance of LDAP Gateway is detected or if you select **No** on the Previous Installation Detected screen, then specify the location where the LDAP Gateway must be installed.
 - a. For Linux
When you install the gateway as a normal user, the default location is inside the Home folder (`home/ubuntu/IDFLDAPGateway-6`).
When you install the gateway as a sudo or root user, the default location is `/opt/IDFLDAPGateway-6`.

- b. For Windows, the default location is Program files (... \ProgramFiles (x86) \IDFLDAPGateway-6)

 **Note:**

If the installation directory points to a location containing an existing gateway, that gateway is automatically upgraded during the installation process.

7. Click **Forward** to proceed.
You are prompted for the license file.
8. Browse to the location containing the **license.lic** file, select it and click **OK**.
The **Ready to Install** window is displayed.
9. Click **Forward** to proceed.
The Installing window is displayed.
10. Once the installation or upgrade is complete, click **View Readme File** to view the changes in the release version.
11. Click **Finish** to complete the installation or upgrade process.

Configuring the LDAP Gateway

Configure the LDAP gateway to connector to the target system and access the data.

The following topics describe the procedure to configure the LDAP Gateway:

 **Note:**

The following procedures are for a fresh installation only. If you already have a running setup or if you want to upgrade, then you do not have to perform these procedures.

- [Creating a Connector Configuration](#)
- [Editing the System Administrator Credentials for Target](#)
- [Configuring the LDAP Gateway with Multiple Connectors](#)
- [Overriding the System Configuration](#)
- [Configuring the Adapter](#)

Creating a Connector Configuration

To allow IDF Gateway to work with a target system, it must be configured for the type of connector and its related parameters for the operations.

Perform the following steps to create a connector configuration:

1. Open the `customer-configuration.properties` file from the `conf/` folder in a text editor to configure the connectors. Copy the connector specific configurations to this file. Refer to the `customer-configuration.properties.example` file from the `conf/` folder to get the connector specific configuration properties. Each connector comes with an example configuration that can be found in the `customer-configuration.properties.example` file. Find the connector definition that you want to turn on and copy that definition in the `customer-configuration.properties` file.

For more information and example settings, see the `customer-configuration.properties` file.

For CA ACF2, copy the following and paste it in the `customer-configuration.properties` file:

```
cnctr.acf2.class=com.identityforge.idfserver.backend.acf2.Acf2Module
cnctr.acf2.acf21.schema=schemas
cnctr.acf2.acf21.suffix=dc=acf2,dc=com
cnctr.acf2.acf21.adminUserDN=cn=idfAcf2Admin,dc=acf2,dc=com
cnctr.acf2.acf21.adminUserPassword=idfAcf2Pwd
cnctr.acf2.acf21.altAdminUserDN=cn=oimAcf2Admin,dc=acf2,dc=com
cnctr.acf2.acf21.altAdminUserPassword=oimAcf2Pwd
cnctr.acf2.acf21.configLocation=../conf/acf2.properties
cnctr.acf2.acf21.allowAnonymous=false
cnctr.acf2.acf21.metaBackend=ldapds
cnctr.acf2.acf21.agent=true
cnctr.acf2.acf21.people.multiCallAttributes=userpassword, revoke, revoked, revoke|revokeDate,userpassword|userpassword,userpassword|passwordexpire
```

2. Add following line to the `customer-configuration.properties` file if it is not already there: `cnctr.coreBean.nexus.cachingEnabled = false`

 **Note:**

This step is mandatory. Otherwise, the cache can become stale and any ACF2 Reconcile All Users Task in Oracle Identity Manager will not be able to reconcile data from the ACF2 target system.

3. Save the file.

Editing the System Administrator Credentials for Target

Modify the system administrator credentials to authenticate access with the Gateway.

Perform the following steps to view and modify the system administrator credentials used to authenticate access with the Gateway:

 **Note:**

Sensitive data is automatically encrypted when the LDAP Gateway starts. For more information, see [About Encrypting Data](#).

Edit the `conf/customer-configuration.properties` in an editor and set values for the following:

- `cnctr.<foo>.<foo>1.adminUserDN=cn=idf<Foo>Admin,dc=<foo>,dc=com`
- `cnctr.<foo>.<foo>1.adminUserPassword=idf<Foo>Pwd`

 **Note:**

- Replace the terms `<foo>` and `<Foo>` with connector specific values. For example, replace `<foo>` with `acf2` and `<Foo>` with `Acf2` for the ACF2 connector.
- While setting the `adminUserDn`, it is mandatory to use `cn` as the RDN identifier.
- If you put spaces after the commas in the DN, you must match that when using that ID to connect to the LDAP Gateway.
- After you modify the `customer-configuration.properties` file, make sure you restart the LDAP Gateway Server to have the changes take effect.

For example, the required format for ACF2 is: `cn=adminId,dc=acf2,dc=com` (the `dc=acf2,dc=com` must match the suffix property).

Configuring the LDAP Gateway with Multiple Connectors

The same type of connector can be instantiated multiple times to represent multiple different endpoints of the same target system. This is, in addition, to the gateway supporting the ability to run various kinds of connectors within a single gateway instance.

It is assumed that you have already configured a single instance of your connector and wish to configure an additional instance. For more information on configuring the LDAP Gateway with a single connector, see [Configuring the LDAP Gateway](#).

To configure the LDAP Gateway with multiple connectors, do the following:

1. In a text editor, open the `customer-configuration.properties` file located in the `conf/` folder for editing.
2. Copy the connector-specific configurations from the `customer-configuration.properties.example` file to the `conf/customer-configuration.properties` file.

For example, copy the following snippet to the `/conf/customer-configuration.properties` file:

```
cnctr.<foo>.class=com.identityforge.idfserver.backend.<foo>.<Foo>Module
cnctr.<foo>.<foo>1.schema=schemas
cnctr.<foo>.<foo>1.suffix=dc=<foo>,dc=com
cnctr.<foo>.<foo>1.adminUserDN=cn=idf<Foo>Admin,dc=<foo>,dc=com
cnctr.<foo>.<foo>1.adminUserPassword=idf<Foo>Pwd
```

```
cnctr.<foo>.<foo>1.altAdminUserDN=cn=oim<Foo>Admin,dc=<foo>,dc=com
cnctr.<foo>.<foo>1.altAdminUserPassword=testpass
cnctr.<foo>.<foo>1.configLocation=../conf/<foo>.properties
cnctr.<foo>.<foo>1.allowAnonymous=false
cnctr.<foo>.<foo>1.defaultUacc=read
cnctr.<foo>.<foo>1.metaBackend=ldapds
cnctr.<foo>.<foo>1.agent=true
```

 **Note:**

Replace the term `<foo>` and `<Foo>` with connector specific values. For example, for ACF2 replace `<foo>` with `acf2` and `<Foo>` with `Acf2`. For more information, see the `customer-configuration.properties.example` file located in the `<LDAP_INSTALL_DIR>/ldapgateway/conf/` directory..

3. In the `/conf/customer-configuration.properties` file, rename the instance ID for the pasted entries if the connector is already defined. For example, rename `acf21` to `acf22`.
4. Modify the following properties as required:
 - `adminUserPassword` - change this for security reasons.
 - `suffix` - represents a unique baseDN. For example, `dc=<foo>dev,dc=com`.
 - `adminUserDN` - full DN of the administrative user account that can use the connector for performing reconciliation and provisioning operations. DN suffix must match the value supplied for `suffix`.
 - `altAdminUserDN` - DN suffix must match the value supplied for `suffix`.
 - `configLocation` - location of the connector property file - e.g. `conf/<foo>.properties`. If the intent is to point these two connector instances to different target systems, the `configLocation` param should point to a different connector properties file for each connector instance. The new properties file can be a copy of the original properties file with changes in the necessary properties to point to the new system.
5. Save the `customer-configuration.properties` file after the configurations are defined.
6. Restart the LDAP Gateway to have the changes take effect.

Overriding the System Configuration

You can override the default system configurations for several reasons. For example, you may want to change the default passwords for the system backend persistence store or change the listening port when the default collides with another service or when the policies of the company require using a different port.

To change the default system properties, locate that property in the `configuration.properties` file (located in the `conf/` folder) and copy it to `customer-configuration.properties` file and provide a new value.

 **Note:**

Not all properties can be modified and must be done in consultation with Support.

To change the default system backend passwords, open the `customer-configuration.properties` file (located in the `conf/` folder) and specify values for the following entries:

```
cnctr.proxy.ldapds.adminUserPassword=<admin-password>
cnctr.proxy.ldapds.altAdminUserPassword=<alt-admin-password>
```

In the preceding snippet, replace `<admin-password>` with the desired password and `<alt-admin-password>` with the desired alternative password for accessing the system backend (`dc=system,dc=backend`).

To change the default port, open the `customer-configuration.properties` file (located in the `conf/` folder) and specify values for the following entries:

```
system.port=6389
system.ssl_port=7389
```

Replace `6389` with the desired listening port for LDAP and `7389` with the desired port for LDAPS.

 **Note:**

- Any of the values defined in `conf/configuration.properties` can be re-defined in `conf/customer-configuration.properties`. Copy the value from `conf/configuration.properties` to `conf/customer-configuration.properties` and modify the value accordingly.
- You must not edit `conf/configuration.properties` directly as it will be overwritten when upgrading.

Configuring the Adapter

To configure the adapter, do the following:

1. Create a `acf2.properties` file in the `conf` folder by renaming the `acf2.properties.example` file located inside the `<LDAP_INSTALL_DIR>/ldapgateway/conf` folder.
2. In a text editor, open the `acf2.properties` file. Edit, specify, and verify that the host, port, user credentials, and other properties are correctly updated to match your environment: The following properties can be configured:

- **Host** – Host name or IP address to connect to the Pioneer Agent. For example, `_host_=localhost`.
- **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. For example, `_port_=5790`.
- **defaultDelete** – Specifies if the user is to be disabled or deleted as an outcome of the **Delete User** provisioning operation. Accepted values are `revoke` or `delete`.

 **Note:**

- To disable the user on the target system as the outcome of the Delete User provisioning operation, set the value of this property to `revoke`. For example, `_defaultDelete_=revoke`.
- To delete the user from the target system as the outcome of the Delete User provisioning operation, set the value of this property to `delete`. For example, `_defaultDelete_=delete`.

- **secretKeyValue** - Specifies the secret key to connect to the MF ACF2. For example, `_secretKeyValue_=`.
- **credentials.username** and **credentials.password** - Credentials to pass to Pioneer as part of authentication enforcement of the connection. Required if the `EnforceAuthentication` flag is set on the pioneer side.
- **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 messages using this port. This value should match the value of the PORT parameter in the Voyager agent control file. For example, `_agentport_=5791`.
- **stcID** - 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). For example, `_stcID_=PIONEERN`.
- **internalEnt** - This property is used to allow the real-time agent to store users in the LDAP internal store. Values are true or false.
- **domainOU** - This property is used to store user in a certain location under the `ou=People` tree of the internal LDAP. This needs to be unique and specific for each system if multiple systems are used within one LDAP Gateway. Default setting is `_domainOu=acf2`.

 **Note:**

ACF2 now supports a new OU called ResourceXRef. It represents the secondary Auth Ids that users can be included and excluded from. The new LDAP attributes represent assignment: "includeids", "includedns", "excludeids", and "excludedns". All these attributes can be used to add and remove users to and from. There must exist at least one include user. However, exclusions can be an empty list.

- **username=** and **password=** - MF is set to authenticate using `auth_ldap = Y` and the `EnforceAuthentication` flag is set on the pioneer side. The credentials are required to pass the Pioneer as part of authentication enforcement of the connection.

 **Note:**

- If you set the value of this property to `No`, then there would be no authentication.
- If you set the value of this property to `Yes`, then it is mandatory to define credentials.

For example, `username=<Acf2 User>` and `credentials.password=<Password>`

- **Error message signature XML** - This file contains error message signatures. The file path is specified in `errormsg-sig-file=`.

```
Define an error message signature XML file that contains new
error message signatures
# (or overrides existing error message signatures by specifying
the same id).
#
#The format of the file should follow
# <Signatures>
#   <Signature id="[unique id]" regex="[regex]" enabled="yes|
no">
#       <!-- Optional Exceptions to reduce false positives -->
#       <Exception regex="[regex]"/>
#       :
#   </Signature>
#   :
# </Signatures>
#
# Value: File path (relative to the folder where the gateway
was executed in)
errormsg-sig-file=
```

- **nameFormat** - Name format for reconciliation. For example, `_nameFormat_=fn|sp|ln`.

To specify the components of the format:

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

Configuring Windows Service

The Windows Service for the LDAP Gateway is installed with a supplied IdentityForge batch file.

The Windows Service installer uses the Apache Procrun utility `prunsvr.exe` to create a fully managed Windows Service for the LDAP Gateway. For more information about Procrun, see <http://commons.apache.org/proper/commons-daemon/procrun.html>.

- [Installing and Configuring the Windows Service for the LDAP Gateway](#)
- [Uninstalling the Windows Service for the LDAP Gateway](#)
- [Configuring Memory Pool Settings](#)

Installing and Configuring the Windows Service for the LDAP Gateway

To install and configure the Windows service for the LDAP Gateway:

1. Open a command prompt (`cmd`).
2. From the command line, execute the command `IDF_Win_Service install` in the `win_service/` directory.
3. Once the service is installed, you can start, stop, and restart it from the standard Windows Services manager or from the command prompt. For example,

```
> net start IdentityForgeService
> net stop IdentityForgeService
```

Note:

If there are any problems with the installation of the service from the batch file, uncomment the `CG_PATH_TO_JVM` variable and ensure that the path is accurate.

```
> rem -- 7. Set this if you want to use a different JVM than the one
> rem set CG_PATH_TO_JVM=C:\Program
> rem set CG_PATH_TO_JVM=C:\Program
Files\Java\jre7\bin\server\jvm.dll
```

If any modifications are required, it is recommended to uninstall the service, make the modifications, and then re-install the service until it installs and runs correctly.

Uninstalling the Windows Service for the LDAP Gateway

To uninstall the Windows service for the LDAP Gateway:

1. Open a command prompt (`cmd`)

2. From the command line, execute the command `IDF_Win_Service remove` in the `win_service/` directory.

Configuring Memory Pool Settings

You can configure the memory pool size for the Windows service by setting values for the `CG_JVMMS` and `CG_JVMMX` variables in the `LDAP_INSTALL_DIR/win_service/IDF-Win-Service.bat` file.

By default, the `CG_JVMMS` and `CG_JVMMX` variables are set to 1024 MB and 2048 MB, respectively. If the LDAP gateway processes a large number of records, then you might encounter the "Out of memory" exception. In such a scenario, you can allocate higher memory for your Windows service by increasing the values of the `CG_JVMMS` and `CG_JVMMX` variables.

To do so:

1. Stop the LDAP gateway Windows service and then uninstall it.
2. In a text editor, open the `LDAP_INSTALL_DIR/win_service/IDF-Win-Service.bat` file for editing.
3. Set the JVM minimum and maximum values by modifying values for the following lines:

```
rem Initial memory pool size in MB.  
set CG_JVMMS=1024
```

```
rem Maximum memory pool size in MB.  
set CG_JVMMX=2048
```

Note:

When you receive the "Out of memory" exception, start with increasing the minimum and maximum values to 2048 and 4096, respectively. If the number of records is greater than 40k, then use higher minimum and maximum values.

4. In the `LDAP_INSTALL_DIR/conf/log4j.properties` file, set the gateway debug level to `ERROR` as follows:

```
rootLogger.level = ERROR
```

5. Install the LDAP gateway Windows service.
6. Start the LDAP gateway through the Windows service.

Starting the LDAP Gateway

1. To start the LDAP Gateway, do one of the following:
 - Execute the `run.bat` script on Windows or `run.sh` on Linux.
 - Start the configured Windows Service.

- Use the shortcut from the Start Menu.
- Double-click the Desktop shortcut.

The LDAP Gateway begins its startup sequence and eventually displays a banner representing the version of the gateway. This banner symbolizes that the gateway is now ready to receive LDAP requests.

2. Check the connection using an LDAP browser with the following connection information:
 - Port: 6389
 - Base DN: `dc=system,dc=backend`
 - User DN: `cn=Directory Manager,dc=system,dc=backend`
 - Password: `testpass`

4

Connector Deployment on Oracle Identity Manager

You must deploy the ACF2 connector locally in 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:

- [Files and Directories in the CA_ACF2_Connector.zip](#)
- [Running the Connector Installer](#)
- [Configuring the IT Resource](#)
- [Configuring Oracle Identity Manager](#)
- [Enabling Logging](#)

Files and Directories in the CA_ACF2_Connector.zip

This zip file contains the connector artifacts that need to be installed in Oracle Identity Manager.

Table 4-1 Files and Directories in the CA_ACF2_Connector.zip

Files in the Installation Media Directory	Description
configuration/ACF2Adv.xml	This XML file contains configuration information that is used during connector installation.
Files in the resources directory	Each of these resource bundles contains locale-specific information that is used by the connector. Note: A resource bundle is a file containing localized versions of text strings that are displayed on the Administrative and User Console. These text strings include GUI element labels and messages. During connector installation, this file is copied to the location, Oracle Identity Manager database.
lib/acf2-provisioning-adapter.jar	This JAR file contains the code for the adapters that are used during connector operations. During connector installation, this file is copied to the following location: Oracle Identity Manager database.
lib/acf2-scheduled-tasks.jar	This JAR file contains the code for the scheduled task that is used during full reconciliation. During connector installation, this file is copied to the following location: Oracle Identity Manager database.

Table 4-1 (Cont.) Files and Directories in the CA_ACF2_Connector.zip

Files in the Installation Media Directory	Description
xml/oimAcf2AdvConnector.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.

Running the Connector Installer

When you run the Connector Installer, it automatically copies the connector files to directories in Oracle Identity Manager, imports connector XML files, and compiles adapters used for provisioning.

To run the Connector Installer:

1. Copy the contents of the connector installation media directory (CA_ACF2_Connector.zip) into the following directory: *OIM_HOME/server/ConnectorDefaultDirectory*

 **Note:**

In an Oracle Identity Manager cluster, copy the entire installation media to each node of the cluster.

2. Log in to the Administrative and User Console by using the user account described in the Creating the User Account for Installing Connectors of *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager*.
3. On the Welcome to Identity Manager Advanced Administration page, in the System Management region, click **Install Connector**.
4. From the Connector List, select **CA ACF2 Adv 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 list, click **Refresh**.
 - c. From the Connector List list, select **CA ACF2 Adv 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. 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. See [Configuring the IT Resource](#).

- c. Configuring the scheduled task that is created when you installed the connector

Record the name of the scheduled task displayed on this page.

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 [Files and Directories in the ACF2 Connector Installation Media](#)

 **Note:**

While installing Oracle Identity Manager in a cluster, you must copy all the JAR files and the contents of the connectorresources directory into the corresponding directories on each node of the cluster. See [Files and Directories in the CA_ACF2_Connector.zip](#) for information about the files that you must copy and their destination locations on the Oracle Identity Manager server.

Configuring the IT Resource

The IT resource for the target system contains connection information about the target system. Oracle Identity Manager uses this information for reconciliation and provisioning.

You must specify values for the parameters of the Acf2Resource IT resource as follows:

1. Log in to the Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Advanced Administration page, in the Configuration region, click **Manage IT Resource**.
3. In the IT Resource Name field on the Manage IT Resource page, enter `Acf2Resource` and then click **Search**.

4. Click the edit icon for the IT resource.
5. From the list at the top of the page, select **Details and Parameters**.
6. Specify values for the parameters of the IT resource. [Table 4-2](#) describes each parameter.

Table 4-2 IT Resource Parameter

Parameter	Description
AtMap User	This parameter holds the name of the lookup definition containing attribute mappings that are used for provisioning. Value: <code>AtMap.ACF2</code> Note: You must not change the value of this parameter.
idfbackendContext	Enter the root context for LDAP Gateway backend. Sample value: <code>dc=system,dc=backend</code>
idfBackendDn	Enter the user ID that the connector will use to connect to the LDAP Gateway backend. Sample value: <code>cn=Directory Manager,dc=system,dc=backend</code>
idfBackendPassword	Enter the password of the user ID that the connector will use to connect to the LDAP Gateway backend. You also set this password in the <code>configuration.properties</code> file of the LDAP Gateway. Note: Do not enter an encrypted value.
idfPrincipalDn	Set a user ID for an account that the connector will use to connect to the LDAP Gateway. Format: <code>cn=USER_ID,dc=acf2,dc=com</code> Sample value: <code>cn=idfAcf2Admin,dc=acf2,dc=com</code> You also set this user ID in the following file: <code>customer-configuration.properties</code> file in <code>LDAP_GATEWAY_HOME/conf</code> directory. See Step 6 in 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 <code>idfPrincipalDn</code> parameter. Note: Do not enter an encrypted value.
idfRootContext	This parameter holds the root context for CA ACF2. Value: <code>dc=acf2,dc=com</code> Note: You must not change the value of this parameter.
idfServerHost	This parameter holds the host name 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. Value: <code>localhost</code> 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.

Table 4-2 (Cont.) IT Resource Parameter

Parameter	Description
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 6 in Installing and Configuring the LDAP Gateway .
idfSsl	This parameter determines whether the LDAP Gateway will use SSL to connect to the target system. Enter <code>true</code> if using SSL. Otherwise, enter <code>false</code> . Sample value: <code>true</code>
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. Sample value: <code>../conf/idf.jks</code>
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: <code>jks</code>
Last Modified Time Stamp	The most recent start time of the Reconcile LDAP Users reconciliation scheduled task is stored in this parameter. See Reconciling Internal LDAP Users to Oracle Identity Manager for more information about this scheduled task. The format of the value stored in this parameter is as follows: <code>MM/dd/yy hh:mm:ss a</code> In this format: <ul style="list-style-type: none"> • 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: <code>05/07/10 02:46:52 PM</code> 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.

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

Configuring Oracle Identity Manager

You must create a UI form and an application instance for the resource against which you want to perform reconciliation and provisioning operations.

The following topics describe the procedures to configure Oracle Identity Manager:

- [Creating and Activating a Sandbox](#)
- [Creating a New UI Form](#)
- [Creating an Application Instance](#)
- [Publishing a Sandbox](#)
- [Updating an Existing Application Instance with a New Form](#)

Creating and Activating a Sandbox

You must create and activate a sandbox to begin using the customization and form management features. You can then publish the sandbox to make the customizations available to other users.

See *Managing Sandboxes in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for instructions on creating and activating a sandbox.

Creating a New UI Form

See *Managing Forms in Oracle Fusion Middleware Administering Oracle Identity Manager* for instructions on creating a new UI form. While creating the UI form, ensure that you select the resource object corresponding to the ACF2 connector that you want to associate the form with.

Creating an Application Instance

Create an application instance and associate it with form created in [Creating a New UI Form](#). For detailed instructions, see the *Managing Application Instances in Oracle Fusion Middleware Administering Oracle Identity Manager*.

Publish the application instance to an organization to make the application instance available for requesting and subsequent provisioning to users. See *Managing Organizations Associated With Application Instances in Oracle Fusion Middleware Administering Oracle Identity Manager* for detailed instructions.

Publishing a Sandbox

You must publish the sandbox that you created in [Creating and Activating a Sandbox](#) to merge the customizations it contains with the main line.

See *Publishing a Sandbox in Oracle Fusion Middleware Developing and Customizing Applications for Oracle Identity Manager* for instructions on publishing a sandbox.

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 [Creating and Activating a Sandbox](#).
2. Create a new UI form for the resource as described in [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 [Publishing a Sandbox](#).

Enabling Logging

When you enable logging, Oracle Identity Manager automatically stores in a log file information about events that occur during the course of provisioning and reconciliation operations. 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:

- ERROR:1
- WARNING:1
- NOTIFICATION:1
- NOTIFICATION:16
- TRACE:1
- TRACE:16
- TRACE:32

See Message Types and Levels in *Oracle Fusion Middleware Administering Oracle Identity Manager* for more information about the log levels.

Oracle Identity Manager level logging operations are managed by the `logging.xml` file which is located in the following directory:

```
DOMAIN_NAME/config/fmwconfig/servers/SERVER_NAME/
```

Loggers are used to configure logging operations for the Oracle Identity Manager functions of the connector.

To configure loggers:

1. In a text editor, open the `DOMAIN_NAME/config/fmwconfig/servers/SERVER_NAME/logging.xml` file.
2. Locate the logger you want to configure. If you are adding a logger for the first time, you must create the logger definition. [Table 4-3](#) lists the Oracle Identity Manager loggers for this connector.

Table 4-3 Logger Parameters

Logger	Description
com.identityforge.util.acf2.LdapOperationsImpl	Logs events related to basic LDAP functions, including connecting to and disconnecting from the LDAP gateway.
com.identityforge.util.acf2.tasks.DeleteReconcileOIMUsersTask	Logs events related to the ACF2 Delete OIM Users scheduled task.
com.identityforge.util.acf2.tasks.FindAllAccessRulesTask	Logs events related to the ACF2 Find All Access Rules scheduled task.
com.identityforge.util.acf2.tasks.FindAllResourcesTask	Logs events related to the ACF2 Find All Resources scheduled task.
com.identityforge.util.acf2.tasks.ReconcileAllLdapUsersTask	Logs events related to the ACF2 Resources scheduled task.
com.identityforge.util.acf2.tasks.ReconcileAllUsersTask	Logs events related to the ACF2 Reconcile All Users scheduled task.

5

Using the Connector

You can use the connector for performing reconciliation and provisioning operations after configuring it to meet your requirements.

This chapter discusses the following topics:

- [Guidelines on Using the Connector](#)
- [Performing Full Reconciliation](#)
- [Performing Filtered \(Limited\) Reconciliation](#)
- [Reconciling Internal LDAP Users to Oracle Identity Manager](#)
- [Reconciling Deleted Users to Oracle Identity Manager](#)
- [Configuring Resource and Access Rule PrePopulation Scheduled Tasks](#)
- [Reconciling Internal LDAP Users to Oracle Identity Manager](#)
- [Uninstalling the Connector](#)

Guidelines on Using the Connector

These are the guidelines that you apply 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 connector can accept and transmit any non-ASCII data to the mainframe, but the mainframe does not accept non-ASCII characters. As a result, any task that requires non-ASCII data transfer fails. In addition, there is no provision in the connector to indicate that the task has failed or that an error has occurred on the mainframe. To avoid errors of this type, you must exercise caution when providing inputs to the connector for the target system, especially when using a regional language interface.
- Passwords used on the mainframe must conform to stringent rules related to passwords on mainframes. These passwords are also subject to restrictions imposed by corporate policies and rules about mainframe passwords. Keep in mind these requirements when you create or modify target system user profiles through provisioning operations on Oracle Identity Manager.

Performing 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.

The ACF2 Reconcile All Users scheduled task performs full reconciliation. When you configure this scheduled task, it runs at specified intervals and fetches create and modify events on the target system for reconciliation.

To configure the Reconcile All Users scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
 - a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
 - b. On the left pane, 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.
 - c. In the search results table on the left pane, click the **scheduled job** in the Job Name column.
4. Modify the details of the scheduled task as follows:
 - On the Job Details tab, 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.

 **See Also:**

Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager for detailed information about schedule types

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

5. Specify values for the attributes of the scheduled task as follows:

 **Note:**

Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

On the Job Details tab, in the Parameters region, specify values for the attributes of the scheduled task. [Table 5-1](#) describes the attributes of the scheduled task.

Table 5-1 Attributes of the 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: Acf2Resource

Table 5-1 (Cont.) Attributes of the Reconcile All Users Scheduled Task

Attribute	Description
Resource Object	Enter the name of the resource object against which reconciliation runs must be performed. Sample value: OIMAcf2ResourceObject
MultiValuedAttributes	Enter a comma-separated list of multivalued attributes that you want to reconcile. Do not include a space after each comma. Sample value: privileges
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, the design form of Oracle Identity Manager allows entering only 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.
Tso Attributes	Enter comma-separated list of tsoattributes of type string. Sample value: tsoDftPfx, tsoAcctNum, tsoProc, tsoSize, tsoRba
TsoBooleanAttributes	Enter comma-separated list of TSO Boolean attributes. Sample value: tsoMail, tsoAcctPriv, tsoAllCmds, tsoJcl, tsoWtp, tsoFscrn, tsoMount
TsoLgnBooleanAttributes	Enter comma-separated list of TSO LOGON Boolean attributes. Sample: tsoLgnAcct, tsoLgnMsg, tsoLgnPerf, tsoLgnProc, tsoLgnTime, tsoLgnRcvr
UsersList	Enter a comma-separated list of user IDs to be reconciled. Note: This attribute is optional. If you do not enter any user IDs, then the connector performs full reconciliation. Sample value: testusr1, testusr2, testusr3
UID Case	Enter lower case if OIM accounts to be reconciled should be in lower case, otherwise enter upper case. Sample value: lower

- After specifying the attributes, click **Apply** to save the changes.

 **Note:**

The Stop Execution option is available in the *Oracle Fusion Middleware User's Guide for Oracle Identity Manager*. You can use the Scheduler Status page to either start, stop, or re-initialize the scheduler.

Performing Filtered (Limited) Reconciliation

You can perform limited reconciliation by creating filters for the reconciliation module, and reconcile records from the target system based on a specified filter criterion.

You might have created multiple resource objects to represent multiple user types in your organization. You use the Resource Object attribute of the Reconcile All Users scheduled task to specify the resource object that you want to use during reconciliation. You can enter more than one resource object in the value of the Resource Object property. In addition, you can include CA ACF2 attribute-value pairs to filter records for each resource object.



See Also:

[Performing Full Reconciliation](#) for information about the Reconcile All Users scheduled task

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

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

As shown 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. 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 Object attribute:

- The names of the resource objects must be the same as the names that you specified while creating the resource objects by using the Design Console.
- The CA ACF2 attribute names must be the same as the names used in the LDAP Gateway configuration files.



See Also:

[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` methodology of the regex matcher is used rather than the `matches` methodology. This means that a substring matching rule can be specified in the pattern, rather than requiring the entire string matching rule.
- 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 Object attribute:

```
(tsoProc:X)ACF2R01, (active:value1|value2|value3)ACF2ResourceObject2,  
(tso)ACF2ResourceObject24000, Resource
```

In this sample value:

- (tsoProc:X)ACF2R01 represents a user with X as the attribute value for the TSO Proc segment. Records that meet this criterion are reconciled with the ACF2RO1 resource object.
- (active:value1|value2|value3)ACF2ResourceObject2 represents a user with value1, value2, or value3 as their active date. Records that meet this criterion are reconciled with the ACF2ResourceObject2 resource object.
- (tso)ACF2ResourceObject24000 represents a user with TSO privileges. A TSO attribute value is not specified. Records that meet this criterion are reconciled with the ACF2ResourceObject24000 resource object.
- All other records are reconciled with the Resource resource object.

Reconciling Internal LDAP Users to Oracle Identity Manager

The ACF2 Reconcile LDAP Users scheduled task allows the administrator 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.

To configure the Reconcile LDAP Users to OIM scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
 - a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
 - b. On the left pane, 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.
 - c. In the search results table on the left pane, click the **scheduled job** in the Job Name column.
4. Modify the following parameters of the scheduled task on the Job Details tab as follows:

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 *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

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

- Specify values for the attributes of the scheduled task as follows:

 **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.

Table 5-2 describes the attributes of the scheduled task.

Table 5-2 Attributes of the Reconcile LDAP Users Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: <code>Acf2Resource</code>
Resource Object	Enter the name of the resource object against which the delete reconciliation runs must be performed. Sample value: <code>OIMAcf2ResourceObject</code>
Domain OU	Enter the name of the internally-configured directory in the LDAP where the contents of event changes will be stored. Sample value: <code>acf2</code>
MultiValuedAttributes	Enter a comma-separated list of multi-valued attributes that you want to reconcile. Do not include a space after each comma. Sample value: <code>privileges</code>
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: <code>uid,owner,defaultGroup,waddr1,tsoMaxSize</code> 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.

Table 5-2 (Cont.) Attributes of the Reconcile LDAP Users Scheduled Task

Attribute	Description
LDAP Time Zone	Enter the time zone ID for the server on which the LDAP gateway is hosted. Sample value: EST, IST
UID Case	Enter whether the user ID should be displayed in uppercase or lowercase. Sample value: upper

- After specifying the attributes, click **Apply** to save the changes.

Reconciling Deleted Users to Oracle Identity Manager

The ACF2 Deleted User Reconciliation to OIM scheduled task allows the administrator to reconcile deleted users from the target system to Oracle Identity Manager.

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.

To configure the Deleted User Reconciliation to OIM scheduled task:

- Log in to the Oracle Identity Manager Administrative and User Console.
- On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
- Search for and open the scheduled task as follows:
 - On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
 - On the left pane, 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.
 - In the search results table on the left pane, click the **scheduled job** in the Job Name column.
- Modify the following parameters of the scheduled task on the Job Details tab as follows:

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 *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

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

- Specify values for the attributes of the scheduled task as follows:

 **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.

Table 5-3 describes the attributes of the scheduled task.

Table 5-3 Attributes of the Deleted User Reconciliation to OIM Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: Acf2Resource
Resource Object	Enter the name of the resource object against which the delete reconciliation runs must be performed. Sample value: OIMAcf2ResourceObject
Domain OU	Enter the name of the internally-configured directory in the LDAP where the contents of event changes will be stored. Sample value: acf2
UID Case	Enter the same value as used in scheduled tasks ACF2 Reconcile All Users and ACF2 Reconcile LDAP Users. Note: If the UID Case value is different from the other jobs, all provisioned accounts might get revoked.

6. After specifying the attributes, click **Apply** to save the changes.

Configuring Resource and Access Rule PrePopulation Scheduled Tasks

The ACF2 Find All Access Rules Task and ACF2 Find All Resource Rules Task scheduled tasks populate lookup tables with resource or access rule keys that can be assigned during user provisioning.

When you configure these scheduled tasks, they run at specified intervals and fetch a listing of all resource or access keys on the target system for reconciliation.

To configure the ACF2 Find All Access Rules Task and ACF2 Find All Resource Rules scheduled task:

1. Log in to Oracle Identity Manager Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:

- a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
 - b. On the left pane, 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.
 - c. In the search results table on the left pane, click the scheduled job in the Job Name column.
4. Modify the following parameters of the scheduled task on the Job Details tab:
- **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.

 **See Also:**

Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager for detailed information about schedule types

5. Specify values for the attributes of the scheduled task as follows:

 **Note:**

Attribute values are predefined in the connector XML file that you import. Specify values only for those attributes that you want to change.

Table 5-4 Attributes of the FindAllAccessRules and FindAllResourceRules Scheduled Tasks

Attribute	Description
IT Resource	Provide the IT Resource name required to fetch the values from the target.

6. After specifying the attributes, click **Apply** to save the changes.

 **Note:**

The Stop Execution option is available in the Oracle Fusion Middleware User's Guide for Oracle Identity Manager. You can use the Scheduler Status page to start, stop, or reinitialize the scheduler.

7. Running the ACF2 Find All Access Rules Task and ACF2 Find All Resource Rules Task populates the lookup tables `Lookup.AccessRuleNames` and `Lookup.ResourceNames` respectively.

 **Note:**

Everytime these tasks are run, the existing lookup values are replaced by the latest values reconciled from the ACF2 target.

Reconciling Internal LDAP Users to Oracle Identity Manager

The ACF2 Reconcile LDAP Users scheduled task allows the administrator 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.

To configure the Reconcile LDAP Users to OIM scheduled task:

1. Log in to the Oracle Identity Manager Administrative and User Console.
2. On the Welcome to Oracle Identity Manager Self Service page, click **Advanced** in the upper-right corner of the page.
3. Search for and open the scheduled task as follows:
 - a. On the Welcome to Oracle Identity Manager Advanced Administration page, in the System Management region, click **Search Scheduled Jobs**.
 - b. On the left pane, 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.
 - c. In the search results table on the left pane, click the **scheduled job** in the Job Name column.
4. Modify the following parameters of the scheduled task on the Job Details tab as follows:

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 *Oracle Fusion Middleware Administrator's Guide for Oracle Identity Manager* for detailed information about schedule types.

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

5. Specify values for the attributes of the scheduled task as follows:

 **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.

Table 5-2 describes the attributes of the scheduled task.

Table 5-5 Attributes of the Reconcile LDAP Users Scheduled Task

Attribute	Description
IT Resource	Enter the name of the IT resource that was configured for the target system. Sample value: <code>Acf2Resource</code>
Resource Object	Enter the name of the resource object against which the delete reconciliation runs must be performed. Sample value: <code>OIMAcf2ResourceObject</code>
Domain OU	Enter the name of the internally-configured directory in the LDAP where the contents of event changes will be stored. Sample value: <code>acf2</code>
MultiValuedAttributes	Enter a comma-separated list of multi-valued attributes that you want to reconcile. Do not include a space after each comma. Sample value: <code>privileges</code>
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: <code>uid,owner,defaultGroup,waddr1,tsoMaxSize</code> 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: <code>EST, IST</code>
UID Case	Enter whether the user ID should be displayed in uppercase or lowercase. Sample value: <code>upper</code>

6. After specifying the attributes, click **Apply** to save the changes.

Uninstalling the Connector

Uninstalling the connector deletes all the account related data associated with resource objects of the connector.

If you want to uninstall the connector for any reason, see *Uninstalling Connectors* in *Oracle Fusion Middleware Administering Oracle Identity Manager*.

6

Extending the Functionality of the Connector

You can extend the functionality of the connector to address your specific business requirements.

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

- [Adding New Attributes for Target Resource Reconciliation](#)
- [Adding New Attributes for Provisioning](#)
- [Removing Attributes Mapped for Target Resource Reconciliation and Provisioning](#)
- [Configuring the Connector for Provisioning to Multiple Installations of the Target System](#)

Adding New Attributes for Target Resource Reconciliation

You can add a new attribute on the process form in the Form Designer section of Oracle Identity Manager System Administration Console.



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 1-3](#) are mapped for reconciliation between Oracle Identity Manager and the target system. If required, you can add new attributes for target resource reconciliation.

The `multiValuedAttributes` property should not be included in the `SingleValueAttributes` property and vice versa. These properties are found in the Reconcile All Users scheduled task.

If you are adding a custom target system attribute, then you must define a new grammar definition in the LDAP gateway for the same. See [About Parsing Grammar Protocol 1.0](#) for more information about new grammar definitions.

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:

- [Adding Custom Fields for Full Reconciliation](#)
- [Adding Custom Fields to Oracle Identity Manager](#)

Adding Custom Fields for Full Reconciliation

You can add custom fields for full reconciliation by specifying a value for the `SingleValueAttributes` attribute of the `Acf2 Reconcile All Users` scheduled task. See [Full and Incremental Reconciliation](#) for more information.

To add a custom field for scheduled task reconciliation:

1. If you are using Oracle Identity Manager 11g R2 PS3 or Oracle Identity Governance 12c, log in to Oracle Identity System Administration.
2. In the left pane, under System Management, click **Scheduler**.
3. Search for and open the **Acf2 Reconcile All Users** scheduled task as follows:
 - a. In the left pane, in the Search field, enter `Acf2 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 `SingleValueAttributes` scheduled task attribute.
5. Click **Apply**.

Adding Custom Fields to Oracle Identity Manager

After adding the custom field to the `ACF2 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 `OIMAcf2ResourceObject` 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 an ACF2 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_ACF2** 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_ACF2_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 **OIMAcf2ProvisioningProcess** 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. For example, from the Field Name field, select Description.
 - e. Double-click the **Process Data field**, and then select **UD_IDF_ACF2_DESCRIPTION**.
 - f. Click **Save** and close the dialog box.
 - g. 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 [Creating a New UI Form](#) and [Updating an Existing Application Instance with a New Form](#).

Adding New Attributes for Provisioning

You can add a new attribute on the process form in the Form Designer section of Oracle Identity Manager System Administration Console.

By default, the attributes listed in [Table 1-3](#) are mapped for provisioning between Oracle Identity Manager and the target system. If required, you can map additional attributes for provisioning.

To add a new attribute for provisioning:



See Also:

Oracle Fusion Middleware User's Guide for Oracle Identity Manager for detailed information about these steps

1. Log in to the Oracle Identity Manager System Administration Console.
2. Add the new attribute on the process form as follows:
 - a. Expand **Development Tools**.
 - b. Double-click **Form Designer**.
 - c. Search for and open the **UD_IDF_ACF2** process form.

- d. Click **Create New Version**, and then click **Add**.
 - e. Enter the details of the attribute.
 - f. Click Save and then click **Make Version Active**.
3. Create an entry for the attribute in the lookup definition for provisioning as follows:
 - a. Expand **Administration**.
 - b. Double-click **Lookup Definition**.
 - c. Search for and open the **AtMap.ACF2** lookup definition.
 - d. Click **Add** and then enter the Code Key and Decode values for the attribute.
The Code Key value must be the name of the field on the process form. The Decode value is the name of the attribute on the target system.
 4. To enable update of the attribute during provisioning operations, create a process task as follows:

 **See Also:**

Oracle Fusion Middleware User's Guide for Oracle Identity Manager for detailed information about these steps

- a. Expand **Process Management**, and double-click **Process Definition**.
- b. Search for and open the **OIMAcf2ProvisioningProcess** 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
 - Allow Cancellation while Pending
 - Allow Multiple Instances
- e. Click **Save**.
- f. On the Integration tab of the Creating New Task dialog box, click **Add**.
- g. In the Handler Selection dialog box, select **Adapter**, click **adpMODIFYACF2USER**, 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:
 - i. Double-click the number of the first row.
 - ii. 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:

Variable Number	Variable Name	Map To	Qualifier
Second	idfResource	IT Resource	Not applicable
Third	uid	Process Data	LoginId
Fourth	attrName	Literal	cn string
Fifth	attrValue	Process Data	UD_ACF2_ADV_NAME string

- j. Click the **Save** icon in the Editing Task dialog box, and then close the dialog box.
 - k. Click the **Save** icon to save changes to the process definition.
5. If you are adding a custom attribute, then add it to the list of attributes specified as the value of the configAttrs property in the Properties in the acf2.properties file. See [Installing and Configuring the LDAP Gateway](#) for information about this property.

Removing Attributes Mapped for Target Resource Reconciliation and Provisioning

You can remove attributes mapped for initial reconciliation.

Note:

You must not remove the uid, cn, sn, givenName, or userPassword attribute. These attributes are mandatory on the target system.

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

Configuring the Connector for Provisioning to Multiple Installations of the Target System

You must create copies of the connector to configure it for multiple installations of the target system.

The following example illustrates this requirement:

The London and New York offices of Example Multinational Inc. have their own installations of the target system. The company has recently installed Oracle Identity Manager, and they want to configure Oracle Identity Manager to link all the installations of the target system.

To meet the requirement posed by such a scenario, you must create copies of the connector. See *Cloning Connectors in Oracle Fusion Middleware Administering Oracle Identity Manager* for more information.

7

Troubleshooting

This chapter provides solutions to problems you might encounter after you deploy the ACF2 connector.

[Table 7-1](#) describes solutions to some problems that you might encounter while using the connector.

Table 7-1 Troubleshooting Tips

Problem Description	Solution
Oracle Identity Manager cannot establish a connection with CA ACF2.	<ul style="list-style-type: none">• Ensure that the mainframe is 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 started. 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 and received.• Examine the Oracle Identity Manager configuration to verify that the IP address, admin ID, and admin password are correct.• Check with the mainframe platform manager to verify that the mainframe user account and password have not been changed.
The mainframe does not appear to respond.	<ul style="list-style-type: none">• Check the connection information that you have provided in the IT resource and the <code>acf2Connection.properties</code> file.• Check the logs. If any of the mainframe JCL jobs have reached an abnormal end, then make the required corrections and rerun the jobs.
A particular use case does not work as expected.	<p>Check for the use case event in the LDAP Gateway logs. Then check for the event in the specific log assigned to the connector:</p> <ul style="list-style-type: none">• If the event has not been recorded in either of these 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 profile, then check for configuration and connections between the LDAP Gateway and the mainframe. <p>Verify that the message transport layer is working.</p>

Table 7-1 (Cont.) Troubleshooting Tips

Problem Description	Solution
The LDAP Gateway fails and stops working	<p>If this problem occurs, then the Reconciliation Agent stops sending messages to the LDAP Gateway. Instead, it stores them in the subpool cache.</p> <p>When this happens, restart the LDAP Gateway instance so that the Reconciliation Agent reads the subpool cache and resends the messages.</p>
The LDAP Gateway is running. However, the Reconciliation Agent fails and stops working	<p>If this problem occurs, then all events are sent to the subpool cache. If the mainframe fails, then all messages are written to the disk.</p> <p>When this happens, restart the Reconciliation Agent instance so that it reads messages from the disk or subpool cache and resends the messages.</p>
The Pioneer STC exits with a SD37 abend	<p>This problem occurred because the dataset sizing for ACF2OUT is incorrect for the number of resource rules used in your environment. This is not a problem with the Pioneer STC, but with your sizing estimates. ACFCMD writes its output to ACF2OUT. As a sizing guideline, a blocksize of 27400 will yield 206 records of 133 bytes each.</p>
The Pioneer STC exits with a S0C4 abend.	<p>This problem possibly occurred because of a conflict between the system settings for the Language Environment (LE) options and what is needed. The LE options that maybe involved are ALL31, HEAP, and STACK. Using a CEEOPTS DD in the job stream may be necessary to override set defaults.</p> <p>See Table 7-2 for the three options settings and their effects.</p>
The PIONEER STC exits with S722 abend when DEBUG=Y is set.	<p>This happens because the debugging output from PIONEER can exceed limits that maybe set for JES2/ JES3 SYSOUT files. Running with DEBUG=Y is meant to be used only on our request for a short duration to troubleshoot an issue. In all other cases DEBUG=N should be used.</p>
Pioneer requires RACF to make calls to R_ADMIN API when the security subsystem is CA-ACF2.	<p>All ACF2 commands are passed through the RACF API interface (service RADMIN, program = IRRSEQ00). Even though the Security Subsystem is CA-ACF2, the RACF API is still used by Pioneer for making calls to R_ADMIN API.</p>

Table 7-1 (Cont.) Troubleshooting Tips

Problem Description	Solution
The PIONEER STC fails with the following error message:	Ensure that you specify a SYSOUT value in the PIONEER CONTROL CARD Setting:
<pre> IKJ56231I FILE AUDTLOG NOT ALLOCATED, SYSTEM OR INSTALLATION ERROR+ IKJ56231I TEXT UNIT X'0018' CONTAINS INVALID PARAMETER AUDIT LOG FAILED TO ALLOC RC: 0056360984 BPXWDYN PARMSTR: ALLOC DD(AUDTLOG) SYSOUT(*) MSG(WTP) </pre>	<p>AUDIT=YES, SYSOUT, CLASS (*)</p> <p>For example: AUDIT=YES, SYSOUT, CLASS(S)</p>

[Table 7-2](#) shows the three options settings and their effects:

Table 7-2 Three Options Settings and their Effects

ALL31	HEAP	STACK	RESULT
OFF	BELOW	BELOW	RC=0
OFF	BELOW	ANYWHERE	Loop
OFF	ANYWHERE	BELOW	S0C4
OFF	ANYWHERE	ANYWHERE	RC=0
ON	BELOW	BELOW	RC=0
ON	BELOW	ANYWHERE	RC=0
ON	ANYWHERE	BELOW	S0C4
ON	ANYWHERE	ANYWHERE	RC=0

A

Files and Directories in the ACF2 Connector Installation Media

These are the components of the connector installation package that comprise the ACF2 connector.

Table A-1 Files and Directories on the Installation Media

File in the Installation Media Directory	Description
CA_ACF2_Connector.zip	This zip contains the connector artifacts that need to be installed in OIM. See Files and Directories in the CA_ACF2_Connector.zip .
ACF2-AGENTS-TIMESTAMP-VERSION.zip	This ZIP file contains the files required to deploy the Reconciliation and Provisioning Agents on the mainframe.
IDF_LDAP_GATEWAY_VERSION.zip	This ZIP file contains the files required to deploy the LDAP Gateway.

B

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

Message: **IDMV000I** Voyager Executing From and APF Authorized Library

Message-Type: Informational

Action Required: None

Description: Module IDFAUTH verified that Voyager is executing out of a APF Authorized Library.

Message: **IDMV000E** Voyager Not Executing From a APF Authorized Library

Message-Type: Severe

Action Required: Voyager Abends

Description: Voyager is being executed from a library that is not APF authorized. To resolve this, APF authorize the Library that Voyager is executing from.

Message: **IDMV000I** Voyager Found RACF|ACF2|TSS Security Subsystem

Message-Type: Informational

Action Required: None

Description: Module IDFIQSEC queried the Security Control Block in Storage And found RACF or ACF2 or Top-Secret, Voyager continues execution.

Message: **IDMV000I** Voyager Found Required Storage Subpool

Message-Type: Informational

Action Required: None

Description: Voyager found the Storage subpool built by STARTUP, Voyager Continues execution.

Message: **IDMV001I** Voyager Input Parameters are OK

Message-Type: Informational

Action Required: None

Description: All parameters passed via PARM= statement were ok no errors

Message: **IDMV002I** Voyager Build Level is at yyyyymmddHHMM - v.r.r.m

Message-Type: Informational

Action Required: None

Description: Voyager Build yyyy = 4 digit year, mm = 2 digit month dd = 2 digit day, HH = 2 digit hour, MM = 2 digit month This was the year,month,day,hour and minute of the Pioneer Reconciliation Agent Production Build prior to Distribution.

Message: **IDMV002I** Oracle Build Level 9.9.9.9.9

Message-Type: Informational

Action Required: None

Description: This is the Oracle Release of Voyager

Message: **IDMV003I** Voyager Subpool 100 BYTE Version

Message-Type: Informational

Action Required: None

Description: This Voyager supports only the 100 Byte version of the Subpool That STARTUP builds.

Message: **IDMV004I** Voyager Detects (TCPIP) Jobname XXXXXXXXX

Message-Type: Informational

Action Required: None

Description: Voyager has detected the TCPIP STC(Started Task) Name where XXXXXXXXX is the STC name passed via the TCPN parameter and used for the connection to the LDAP Gateway.

Message: **IDMP005I** Pioneer Detects (TCPIP) IP Address of xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Description: Voyager will use this IP Address and PORT= to connect to the LDAP Gateway. This IP Address or Hostname is passed via PARM=, IPAD= parameter.

Message: **IDMV006I** Voyager Detects (TCPIP) IP PORT xxxx

Message-Type: Informational

Action Required: None

Description: Voyager will use the PORT= number in conjunction with the IPAD= parameter to connect to the LDAP gateway.

Message: **IDMV007I** Voyager Detects Encryption is ON

Message-Type: Informational

Action Required: None

Description: Voyager via ESIZE=16 will turn on 'enable' AES 128 encryption module for encryption of messages to/from LDAP.

Message: **IDMV008I** Voyager Detects Cache Delay Set to xx Secs

Message-Type: Informational

Action Required: None

Description: Voyager via DELAY= parameter will set a DELAY for polling Cache to xx Secs this is only applicable to CA Top-Secret users only. All other users (RACF and ACF2) should set this Parameter to DELAY=00

Message: **IDMV009I** Voyager Detects Cache File Opened OK

Message-Type: Informational

Action Required: None

Description: Voyager's external Cache file on dasd has opened ok.

Message: **IDMV010I** Voyager Computing Cache Timer Delay successful

Message-Type: Informational

Action Required: None

Description: Voyager computed the DELAY= value correctly and will use it for polling cache. This is only applicable to CA Top-Secret users only.

Message: **IDMV011I** Voyager Detects Encryption KVER xxxxxxxxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: Voyager via ESIZE= parameter passed as a PARM= in the STC is using KVER xxxxxxxxxxxxxxxxxxxx for Encryption.

Message: **IDMV012I** Voyager Detects Debugging is ON

Message-Type: Informational

Action Required: None

Description: Voyager will use the DEBUG= parameter passed to provide detailed diagnostics for Oracle/IDF technical personnel. The output routes to the DEBUGOUT 'DD' statement in Voyager. Be aware if DEBUG=Y then there will be a lot of output placed into the JES2 queue.

Message: **IDMV013I** Voyager Detects Debugging is OFF

Message-Type: Informational

Action Required: None

Description: Voyager will use the DEBUG= parameter passed and no detailed diagnostics will route to the DEBUGOUT 'DD' statement in Voyager.

Message: **IDMV014I** Voyager Detects MVS retcodes of xxx

Message-Type: Informational

Action Required: None

Description: Voyager via the PRTNCRD= parameter passed will use this value for its return code when it is shutdown. The value of 'SHUTRC' will produce a 0000 return code and the value of 'TERMRC' will produce the return code greater than zero and that was contained in register 15 at time of shutdown.

Message: **IDMV015I** Voyager Detects Country Code of XX

Message-Type: Informational

Action Required: None

Description: Voyager has queried z/OS and retrieved the Country code of this system. This will be used in all conversions from EBCDIC to ASCII and ASCII to EBCDIC.

Message: **IDMV016I** Voyager Detects Hostname of xxxxxxxxxxx.xxx

Message-Type: Informational

Action Required: None

Description: Voyager was passed via IPAD= parameter a Hostname instead Of an IP address and this will be used to connect to the LDAP Gateway.

Message: **IDMV016E** Voyager Detects Bad Hostname of xxxxxxxxxxx.xxx

Message-Type: Error

Action Required: Investigate error

Description: Voyager was passed via IPAD= parameter a Hostname instead Of an IP address and this will be used to connect to the LDAP Gateway this Hostname was queried via the local DNS server(s) and failed to be resolved.

Message: **IDMV019I** Voyager Initialization of TCP API was Successful

Message-Type: Informational

Action Required: None

Description: Voyager has initialized the TCPIP stack successfully

Message: **IDMP019E** Voyager Initialization of TCP API Failed RC: xx

Message-Type: Error

Action Required: Investigate error

Description: Voyager's initialization of the TCPIP API interface failed. A primary cause is a missing security subsystem (RACF,ACF2, Or Top-Secret) permit for facility 'bpx.*'

Message: **IDMV020I** Voyager Initialization of GETCLIENTID was Successful

Message-Type: Informational

Action Required: None

Description: Voyager has issued a GETCLIENTID and it was successful. This is normal for the client/socket server like Voyager.

Message: **IDMV021I** Voyager Accepting Messages on xxx.xxx.xxx.xxx (OR) hostname.com

Message-Type: Informational

Action Required: None

Description: Voyager will send/receive message to/from the LDAP gateway on IP Address xxx.xxx.xxx.xxx with PORT= or on Hostname - Hostname.com with PORT= * Note: Hostname.com is an example, this would be the hostname Of the LDAP gateway.

Message: **IDMV021I** Voyager Initialization of PTON was successful

Message-Type: Informational

Action Required: None

Description: Voyager successfully converted the IP address to the correct addressing type to communicate to the LDAP gateway.

Message: **IDMV021E** Voyager Initialization of PTON failed RC: xx

Message-Type: Error

Action Required: Investigate

Description: Voyager failed during its conversion to numeric. The RC(return code) is documented in the following source. z/OS V1R9.0 Communication Server IP CICS Sockets Guide Manual – SC31-8807-04

Message: **IDMV025I** Voyager Connected to Gateway Server was successful

Message-Type: Informational

Action Required: None

Description: Voyager successfully connected to the LDAP Gateway using either IP address = xxx.xxx.xxx.xxx or Hostname.com with PORT = xxxx.

Message: **IDMV032I** Voyager Connection Start Timer Begins

Message-Type: Informational

Action Required: None

Description: Voyager using PARM=, 'STARTDELAY=' will delay it's connection by xx secs specified in 'STARTDELAY='. The STARTDELAY=' timer started.

Message: **IDMV033I** Voyager Connection Start Timer Ends

Message-Type: Informational

Action Required: None

Description: Voyager using PARM=, 'STARTDELAY=' will delay it's connection by xx secs specified in 'STARTDELAY='. The 'STARTDELAY=' timer ended.

Message: **IDMV050I** Voyager Cache Polling Begins

Message-Type: Informational

Action Required: None

Description: Voyager has started polling its subpool 231 cache for events created by the installed product exits. This is a normal process for the real-time reconciliation agent.

Message: **IDMV051I** Voyager Cache Polling Ends

Message-Type: Informational

Action Required: None

Description: Voyager has ended its polling its subpool 231 cache for events created by the installed product exits. This is a normal process for the real-time reconciliation agent.

Message: **IDMV060I** Voyager is OK and Working

Message-Type: Informational

Action Required: None

Description: The Operator queried Voyager's status with a "F stcid,STATUS" command. This message is usually coupled.

Message: **IDMV061I** Voyager is Setting DEBUG to YES

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=Y' command to Voyager

Message: **IDMV062I** Voyager is OK and Working

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=N' command to Voyager

Message: **IDMV063I** Voyager DEBUG is ALL READY ACTIVE

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=Y' and DEBUGGING was All ready active.

Message: **IDMV064I** Voyager DEBUG Will Be Activated

Message-Type: Informational

Action Required: None

Description: The Operator issued a 'F stcid,DEBUG=Y' and Voyager has turned on DEBUGGING.

Message: **IDMV065I** Voyager Debugging is not Active

Message-Type: Informational

Action Required: None

Description: The Operator issued a "F stcid,DEBUG=N" and debugging was already off.

Message: **IDMV100I** Voyager Shutdown Started

Message-Type: Informational

Action Required: None

Description: Voyager Shutdown has started via a z/OS Modify command.

Message: **IDMV101I** Voyager Reconciliation Agent Has Terminated

Message-Type: Informational

Action Required: None

Description: Voyager has been terminated

Message: **IDMV102I** Voyager has Ended with Zero Return Codes

Message-Type: Informational

Action Required: None

Description: Voyager has ended with a zero MVS Condition code. This condition was set with the PRTNCODE=SHUTRC parameter.

Message: **IDMV103I** Voyager has Ended with Non-Zero Return Code

Message-Type: Informational

Action Required: None

Description: Voyager has ended with a non-zero MVS Condition code. This condition was set with the PRTNCODE=TERMRC parameter.

Message: **IDMV104I** Voyager sent messages xxxxxx received messages xxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Description: Voyager shutdown statistic on amount of work done.

Message: **IDMV102E** Voyager Cache Dasd File Not be Found

Message-Type: Error

Action Required: Investigate

Description: Voyager Cache dasd file used for recovery was not found and Voyager will abend.

Message: **IDMV151I** Voyager DNS Request hostname.com

Message-Type: Informational

Action Required: None

Description: Voyager via IPAD= has been asked to use a DNS hostname instead of an IP Address to connect to the LDAP gateway.

Message: **IDMV152I** Voyager IP Connect Request xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Description: Voyager via IPAD= has been asked to use an IP address instead of a hostname to connect to the LDAP gateway.

Message: **IDMV200E** Voyager Startup Parameter Error xxxxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: Voyager had a startup PARM= error, indicated by xxxxxxxxxxxxxxxx

Message: **IDMV200I** Voyager unable to connect to the Gateway

Message-Type: Informational

Action Required: None

Description: Voyager was unable to connect to the LDAP Gateway either via hostname or IP Address, Voyager will retry the connection. This message and IDMV201I usually are together.

Message: **IDMV201I** VoyagerConnection to the Gateway Failed IP=999.999.999.999

Message-Type: Informational

Action Required: None

Description: Voyager was unable to connect to the LDAP Gateway either via hostname or IP Address, Voyager will retry the connection. This message and IDMV200I are usually together, the IP= is the IP Address or Hostname of the LDAP Gateway that Voyager is trying to connect to. Voyager will attempt retries ever 15-20 seconds.

Message: **IDMV202E** Voyager no Storage Token Found

Message-Type: Informational

Action Required: None

Description: Voyager was unable to find the required subpool 231 storage token, Voyager will terminate.

Message: **IDMV202I** Voyager Unable to Connect to new IP/Port

Message-Type: Informational

Action Required: None

Description: Voyager's IP address and port were swapped via a Modify command and it could not connect to the LDAP using that combination.

Message: **IDMV203E** Voyager Quiescing Because of the subpool Not found.

Message-Type: Informational

Action Required: None

Description: Voyager is shutting down because of a missing Storage token for the subpool, required for normal operations.

Message: **IDMV204E** Voyager subpool 231 cannot be found

Message-Type: Informational

Action Required: None

Description: Voyager went to poll the subpool 231 (cache) for events And the subpool was not there. This will result in Voyager Quiescing and shutting down.

Message: **IDMV300I** *Debug* - xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Message-Type: Error

Action Required: None

Description: Voyager will display this statement when DEBUG=Y is on and Output will route to // DEBUGOUT 'DD'.

Message: **IDMV400I** *Status* - xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: Voyager will display a status as it processes RACF events from the subpool.

C

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 Provision Agent is Starting

Message-Type: Informational

Action Required: None

Message: **IDMP001I** Pioneer Input Parameters are OK

Message-Type: Informational

Action Required: None

Description: All parameters passed via PARM= statement were ok no errors

Message: **IDMP002I** Pioneer Detects Build yyyymmddHHMM

Message-Type: Informational

Action Required: None

Description: Pioneer Build yyyy = 4 digit year, mm = 2 digit month dd = 2 digit day, HH = 2 digit hour, MM = 2 digit month. This was the year,month,day,hour and minute of the Pioneer Provisioning Agent Production Build prior to Distribution.

Message: **IDMP003I** Pioneer Detects TCPIP Jobname XXXXXXXX

Message-Type: Informational

Action Required: None

Description: Pioneer has detected the TCPIP STC(Started Task) Name where XXXXXXXX is the STC name passed via the TCPN parameter and used for the connection to the LDAP Gateway.

Message: **IDMP004I** Pioneer Detects TCPIP IP Address of xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Description: Pioneer will not use this IP Address it must be 0.0.0.0, Pioneer is a Socket Server and is only using PORT=, passed by the IPAD= parameter.

Message: **IDMP005I** Pioneer Detects TCPIP IP PORT of xxxx

Message-Type: Informational

Action Required: None

Description: Pioneer will use this port passed in the PORT= parameter to accept connections from the LDAP server. This port does not need reserving in the TCPIP configuration file on z/OS.

Message: **IDMP006I** Pioneer Detects Debugging is ON

Message-Type: Informational

Action Required: None

Description: Pioneer will use the DEBUG= parameter passed to provide detailed diagnostics for Oracle/IDF technical personnel. The output routes to the DEBUGOUT 'DD' statement in Pioneer. Be aware if DEBUG=Y then there will be a lot of output placed into the JES2 queue.

Message: **IDMP007I** Pioneer Detects Debugging is OFF

Message-Type: Informational

Action Required: None

Meaning: Pioneer will use the DEBUG= parameter passed and no detailed diagnostics will route to the DEBUGOUT 'DD' statement in Pioneer.

Message: **IDMP008I** Pioneer Detects KVER xxxxxxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: Pioneer via ESIZE= parameter passed as a PARM= in the STC is using KVER xxxxxxxxxxxxxxxxx for Encryption.

Message: **IDMP009I** Pioneer Detects Encryption Enabled

Message-Type: Informational

Action Required: None

Description: Pioneer via ESIZE=16 will turn on 'enable' AES 128 encryption module for encryption of messages to/from LDAP.

Message: **IDMP010I** Pioneer Detects Encryption Disabled

Message-Type: Informational

Action Required: None

Description: Pioneer via ESIZE=00 will turn off 'disable' AES 128 encryption module for encryption of messages to/from LDAP. Warning, Pioneer will not work in this mode of Operation.

Message: **IDMP011I** Pioneer Detects CPUID xxxxxxxxxxxxx

Message-Type: Informational

Action Required: None

Description: Pioneer has queried z/OS and retrieved the actual CPUID of the system it is running.

Message: **IDMP012I** Pioneer Detects Sysplex Sysname xxxxxxxx

Message-Type: Informational

Action Required: None

Description: Pioneer has queried z/OS and retrieved the actual Sysplex Sysname it is executing on.

Message: **IDMP013I** Pioneer Detects LPARNAME xxxxxxxx

Message-Type: Informational

Action Required: None

Description: Pioneer via the LPAR= parameter will use the xxxxxxxx as A name for this system. This is informational only. Will be used in a later release of software.

Message: **IDMP014I** Pioneer Detects Country Code of XX

Message-Type: Informational

Action Required: None

Description: Pioneer has queried z/OS and retrieved the Country code of this system. This will be used in all conversions from EBCDIC to ASCII and ASCII to EBCDIC.

Message: **IDMP015I** Pioneer Detects Job Wait Time Of xx Secs

Message-Type: Informational

Action Required: None

Description: Pioneer has detected a Job Wait Time Of xx seconds. This is The JWAIT= PARM. Used for an optional feature not supported by all versions of Pioneer or LDAP.

Message: **IDMP015I** Pioneer Detects RECON wait time of xx Mins

Message-Type: Informational

Action Required: None

Description: Pioneer has detected via PARM= a RWAIT= which controls the Amount of time Pioneer waits to query RECON file completion.

Message: **IDMP020I** Pioneer Accepting Messages on xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has initialized the TCPIP stack with its calls and has bound a socket for listening to the PORT= parameter.

Message: **IDMP020A** Pioneer Operator has Issued a Shutdown Command Message-
Type: Informational

Action Required: Action

Meaning: Pioneer has been requested to shutdown via Modify command

Message: **IDMP030I** Pioneer INITAPI was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has Initialized the TCPIP stack successfully

Message: **IDMP031I** Pioneer GETCLIENTID was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has issued a GETCLIENTID and it was successful. This is normal for the socket server like Pioneer.

Message: **IDMP032I** Pioneer CLIENT NAME/ID is xxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully acquired the CLIENTID required for a socket server connection and it will use xxxxxxxx as the name.

Message: **IDMP033I** Pioneer CLIENT TASK is xxxxxxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully acquired the CLIENTID required for a socket server connection and it will use xxxxxxxx as the Task name.

Message: **IDMP034I** Pioneer CREATE SOCKET was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully created a socket for its SOCKET Server function.

Message: **IDMP035I** Pioneer BIND SOCKET was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully BINDED the Socket to the port that was passed via PORT= parameter.

Message: **IDMP036I** Pioneer Listening port is xxxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer will be listening on port xxxx for incoming LDAP requests.

Message: **IDMP037I** Pioneer Listening Address is xxx.xxx.xxx.xxx

Message-Type: Informational

Action Required: None

Meaning: Pioneer will be listening on IP Address xxx.xxx.xxx.xxx for incoming LDAP requests.

Message: **IDMP038I** Pioneer Listen Socket Call was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has successfully issued a Socket Listen call.

Message: **IDMP039I** Pioneer Read Socket Call was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received a message from the LDAP gateway via the Read Socket call and it was successful.

Message: **IDMP039I** Pioneer Write Socket Call was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has sent a message to the LDAP gateway via the Write Socket call and it was successful.

Message: **IDMP040I** Pioneer Translation was successful from-to xxxxxxxxxxxxxxxxxxxx.
(ASCII-TO-EBCDIC) or (EBCDIC-TO-ASCII)

Message-Type: Informational

Action Required: None

Meaning: Pioneer successfully translated LDAP's message from ASCII-TO-EBCDIC or translated the message going to The LDAP gateway from EBCDIC-TO-ASCII

Message: **IDMP040E** Pioneer Translation was not successful from-to xxxxxxxxxxxxxxxxxxxx.
(ASCII-TO-EBCDIC) or (EBCDIC-TO-ASCII)

Message-Type: Informational

Action Required: None

Meaning: Pioneer did not successfully translated LDAP's message from ASCII-TO-EBCDIC or the message going to The LDAP gateway from EBCDIC-TO-ASCII

Message: **IDMP040I** Pioneer Socket Accept was successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer's Socket Accept call was successful.

Message: **IDMP040E** Pioneer Socket Accept was not successful RC: xxxxxxxx

Message-Type: Error

Action Required: Review Socket Accept Return Code and take required action as outlined in z/OS V1R9.0 Communication Server IP CICS Sockets Guide – SC31-8807-04

Meaning: Pioneer's Socket Accept call failed with RC: xxxxxxxx

Message: **IDMP048I** Pioneer LDAP Connection Timed out

Message-Type: Informational

Action Required: None

Meaning: Pioneer to LDAP connection timed out.

Message: **IDMP049I** Pioneer Has Been Idle for 30 Mins

Message-Type: Informational

Action Required: None

Meaning: Pioneer has not received any messages from LDAP Gateway in 30 mins.

Message: **IDMP050A** Pioneer Closing IP Connection

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received or issued a Socket Close and the connection will be closed.

Message: **IDMP051I** Pioneer Close Socket Call was Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received or issued a Socket Close and it was successful

Message: **IDMP052I** Pioneer Shutdown Socket Call was Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received or issued a Socket Close and it was successful

Message: **IDMP053I** Pioneer MYRADMIN SAF call was Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer has passed the security system function call via the SAF interface (module IRRSEQ00) and it was a success.

Message: **IDMP054I** Pioneer Received ACF2 Recon Request from LDAP

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received a Batch Recon request from the LDAP Gateway.

Message: **IDMP055I** Pioneer Recon Processing Started

Message-Type: Informational

Action Required: None

Meaning: Pioneer has received a Batch Recon request from the LDAP Gateway and has been submitted to z/OS.

Message: **IDMP056I** Pioneer Recon Processing Ended

Message-Type: Informational

Action Required: None

Meaning: Pioneer Batch Recon request has ended.

Message: **IDMP057I** Pioneer Recon Processing Successful

Message-Type: Informational

Action Required: None

Meaning: Pioneer Batch Recon Request was successful and data was retrieved and send back to the LDAP gateway.

Message: **IDMP058I** Pioneer Recon Has Processed: xxxx Userids

Message-Type: Informational

Action Required: None

Meaning: Pioneer Recon Processing status message. The xxxx is the increment and is usually 1000 userids/ACIDS.

Message: **IDMP058I** Pioneer Recon Total Processed: xxxxxx Userids

Message-Type: Informational

Action Required: None

Meaning: Pioneer Recon Processing status message. The xxxxxx is the total of the processed users/ACIDS and is put out with the first IDMP058I message.

Message: **IDMP070I** Pioneer xxxxxxxx Is Now Open

Message-Type: Informational

Action Required: None

Meaning: Pioneer file xxxxxxxx is now Open.

Message: **IDMP071I** Pioneer xxxxxxxx Is Now Closed

Message-Type: Informational

Action Required: None

Meaning: Pioneer file xxxxxxxx is now Closed

Message: **IDMP070I** Pioneer Could Not Open xxxxxxxx RC: xx

Message-Type: Informational

Action Required: None

Meaning: Pioneer file xxxxxxxx could not be opened

Message: **IDMP080I** Pioneer Job Submitted to the Intrdr

Message-Type: Informational

Action Required: None

Meaning: Pioneer has punched a Job to the Intrdr, see JCLOUTP 'DD' in Pioneer for details.

Message: **IDMP100I** Pioneer (IN) Msgs Processed is xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None Meaning: Pioneer has processed xxxxxxxxxx (IN) bound messages from LDAP gateway.

Message: **IDMP100I** Pioneer (OUT) Msgs Processed is xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxxx (OUT) bound messages To LDAP gateway.

Message: **IDMP100I** Pioneer Message (READ) Bytes xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxxx (IN) bound messages bytes from LDAP gateway.

Message: **IDMP100I** Pioneer Message (WRITE) Bytes xxxxxxxxxx

Message-Type: Informational – Shutdown Statistic

Action Required: None

Meaning: Pioneer has processed xxxxxxxxxx (OUT) bound messages bytes to the LDAP gateway.

Message: **IDMP200E** Pioneer Startup Parameter Error xxxxxxxxxxxxxxx

Message-Type: Error

Action Required: None

Meaning: Pioneer has shutdown with a PARM= error, see SYSOUT 'DD' for the details of the error.

Message: **IDMP300I** *Debug* - xxxxxxxxxxxxxxxxxxxxxxxxxxx

Message-Type: Error

Action Required: None

Meaning: Pioneer will display this statement when DEBUG=Y is on and Output will route to // DEBUGOUT 'DD'.

D

Authorized Libraries

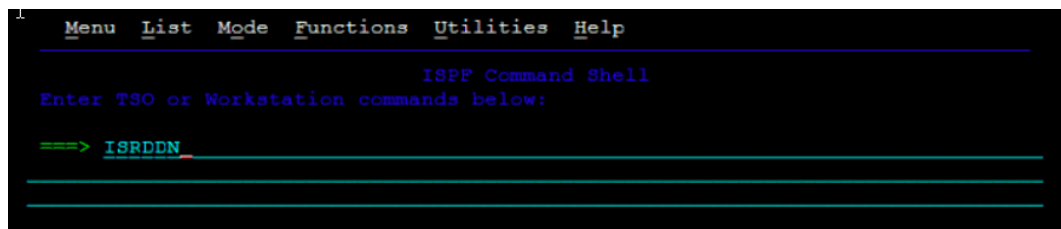
APF means "Authorized Program Facility". In a z/OS environment, APF is a facility that permits the identification of programs that are authorized to use restricted functions. APF-authorized programs must reside in one of the following authorized libraries:

- SYS1.LINKLIB
- SYS1.SVCLIB
- SYS1.LPALIB
- Authorized libraries specified by your installation

Authorized libraries are defined in an APF list, or in the link pack area (LPA). Any module in the LPA (pageable, modified, fixed, or dynamic) will be treated by the system as though it came from an APF-authorized library. The installation must ensure that it has properly protected SYS1.LPALIB and any other library that contributes modules to the link pack area to avoid system security and integrity exposures, just as it would protect any APF-authorized library. 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 that are APF authorized:

1. Type TSO ISRDDN in your ISPF session (some shops need just ISRDDN with no TSO prefix) and hit enter.



```
Menu List Mode Functions Utilities Help
ISPF Command Shell
Enter TSO or Workstation commands below:
=> ISRDDN
```

2. Type APF and hit enter. It'll 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.

```

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 > - AOPPRINT ----- JES2 Subsystem file -----
3CRES2 SHR,KEEP > - AOPTABL  AUT330.AOPTABL
3CRES2 SHR,KEEP > - DITPLIB  DIT130.SDITPLIB
3CPRD2 SHR,KEEP > - IHVCONF  AUT330.IHVCONF
2CSYS1 NEW,DEL > - ISPCTL1  SYS12251.T223906.RA000.MLIGHT.R0100807
2CSYS1 NEW,DEL > - ISPCTL2  SYS12251.T223906.RA000.MLIGHT.R0100808
3CRES2 SHR,KEEP > - ISPEXEC  ISP.SISPEXEC
3CRES1 SHR,KEEP > -          SYS1.SBPXEXEC
3CPRD2 SHR,KEEP > -          CSQ701.SCSQEXEC
3CRES1 SHR,KEEP > -          EUV.SEUVEEXEC
3CRES2 SHR,KEEP > - ISPLLIB  GDDM.SADMMOD
3CRES2 SHR,KEEP > -          FMNA10.SFMMOD1
3CPRD2 SHR,KEEP > -          CSQ701.SCSQAUTH
3CRES2 SHR,KEEP > -          AUT330.SINGMOD1
3CRES1 SHR,KEEP > -          TCPIP.SEZALOAD
2CSYS1 NEW,DEL > - ISPLST1  SYS12251.T223906.RA000.MLIGHT.R0100809
2CSYS1 NEW,DEL > - ISPLST2  SYS12251.T223906.RA000.MLIGHT.R0100810
3CRES2 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
3CRES1 > - APPLIST  SYS1.LINKLIB
3CRES1 > -          SYS1.SVCLIB
3CRES1 > -          SYS1.SHASLNKE
3CRES1 > -          SYS1.SIEMIGE
3CRES1 > -          SYS1.MIGLIB
3CRES1 > -          SYS1.SERBLINK
3CRES1 > -          SYS1.SIEALNKE
3CRES1 > -          SYS1.CSSLIB
3CRES1 > -          GIM.SGIMLMD0
3CRES1 > -          IOE.SIOELMOD
3CRES1 > -          SYS1.SHASMIG
3CRES2 > -          CSF.SCSFMODE
3CRES1 > -          SYS1.SBDTCMD
3CRES1 > -          SYS1.SBDTLIB
2CSYS1 > -          USER.LINKLIB
3CRES1 > -          ADCD.2112.LINKLIB
3CRES1 > -          ADCD.2112.VTAMLIB
2CSYS1 > -          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

```

E

Relationship between the Pioneer (DDs), Voyager (DDs) and the INDDs

Table E-1 shows the relationship between the Pioneer (DDs) and the INDDs in CREATDSN member. Pioneer was used as a High-Level Qualifier to illustrate only.

Table E-1 Relationship between the Pioneer (DDs) and the INDDs in CREATDSN Member

Pioneer DD:	CREATDSN DD:
LISTINR	//INDD1 DD DSN=PIONEER.ALIASOUT, //DCB=(DSORG=PS,RECFM=VBA,LRECL=133,BLKSIZE=0), // UNIT=SYSDA,SPACE=(CYL,5),DISP=(NEW,CATLG), // VOL=SER=??????
IDCAMSD	//INDD2 DD DSN=PIONEER.IDCAMSD.FILE, //DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80 // UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG), // VOL=SER=??????
ACF2CTL	//INDD3 DD DSN=PIONEER.ACF2.CTL, //DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80 // UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG), // VOL=SER=??????
ACF2OUT	//INDD4 DD DSN=PIONEER.ACF2OUT, //DCB=(DSORG=PS,RECFM=VBA,LRECL=133,BLKSIZE=0), // UNIT=SYSDA,SPACE=(CYL,5),DISP=(NEW,CATLG), // VOL=SER=??????
PARMFLE	//INDD7 DD DSN=PIONEER.CONTROL.FILE, //DCB=(DSORG=PS,RECFM=F,LRECL=80,BLKSIZE=80 // UNIT=SYSDA,SPACE=(TRK,5),DISP=(NEW,CATLG), // VOL=SER=??????
NOTES:	Set VOL=SER=?????? to the location of the datasets. If customer is not using SMS to manage space.

 **Note:**

Voyager was used as a High-Level Qualifier to illustrate only.

Table E-2 shows the relationship between the Voyager (DDs) and the INDDs in CREATDSN.

Table E-2 Relationship between the Voyager (DDs) and the INDDs in CREATDSN Member

Voyager DD:	CREATDSN DD:
CACHESAV	//INDD5 DD DSN=VOYAGER.CACHESAV, // DCB=(DSORG=PS,RECFM=FB,LRECL=112,B LKSIZE=27888), // UNIT=SYSDA,SPACE=(CYL,10),DISP=(NEW, CATLG), // VOL=SER=??????
PARMFLE	//INDD6 DD DSN=VOYAGER.CONTROL.FILE, // DCB=(DSORG=PS,RECFM=F,LRECL=80,BLK SIZE=80), // UNIT=SYSDA,SPACE=(TRK,1),DISP=(NEW,C ATLG), // VOL=SER=??????
NOTES:	Change vol=ser to the location of the datasets. If customer is not using SMS to manage space.

Table E-3 describes the purpose of the Pioneer (DDs) and the files that were loaded by CREATDSN.

Table E-3 Purpose of the Pioneer (DDs)

Pioneer (DD):	Purpose:	Size Requirement:
LISTINR	Output file of the INJCLR JCL execution. Pioneer reads this file and sends it back to the LDAP.	None, this file is large enough.
IDCAMSD	IBM's IDCAMS control file Parameters sent by the LDAP.	No more than 2 Trks.
ACF2CTL	CA ACF2's internal SYSIN file For parameters sent by LDAP Input into the ACF2 call.	No more than 2 Trks.
ACF2OUT	CA ACF2's internal SYSPRINT file output of ACF2 calls.	No more than 2 Trks.
JCLOUTP	Output SYSOUT file for all listings of submitted JCL	N/A
AUDTLOG	Output SYSOUT file for AUDIT listings when the PARMFLE parameter AUDIT=YES is on.	N/A