

**Oracle® Communications Session Delivery
Manager**
Administration Guide
Release 7.5

August 2016

Notices

Copyright© 2016, 2016, Oracle and/or its affiliates. All rights reserved.

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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

About This Guide	5
Revision History.....	6
1 Health Monitor	9
Overview.....	9
Accessing the Health Monitor Console.....	9
Heartbeat Monitor.....	10
Disk Usage.....	11
Summary.....	11
Details.....	13
2 Security Manager	15
Configure External User Authentication.....	15
Configure a RADIUS Server.....	16
Configure an Active Directory Domain Controller.....	17
Configure Groups.....	18
Find an External Domain User Group.....	18
Add and Map a Local User Group to an External Domain User Group.....	19
Add a Local User Group.....	20
Delete a User Group.....	21
Change Privileges for User Groups.....	21
Operations Tree Structure.....	22
Apply User Group Privileges for the Administrative Operations.....	22
Apply User Group Privileges for Fault Management Operations.....	24
Apply User Group Privileges for Applications.....	24
Apply User Group Privileges for Product Configurations.....	25
Apply User Group Privileges for Session Border Controller System Boot Parameters.....	27
Apply User Group Privileges for Device Groups.....	27
Configure Users.....	28
Add a User.....	28
Edit a User.....	29
Reactivate a User.....	30
Delete a User.....	31
Reset a User Password.....	31
Change a User Password.....	31
Change User Password Rules.....	31
Notify When to Change the User Password.....	32
Set the Inactivity Timer to Prevent Unauthorized System Access.....	33
Audit Logs.....	33
View and Save an Audit Logs.....	33
Search the Audit Log.....	34
Schedule Audit Log Files to Be Purged Automatically.....	35
Purge Audit Log Files Manually.....	35
3 Northbound Interface	37
Northbound Fault Management.....	37
Accessing Northbound Fault Management Configuration.....	39
X.733 Traps to SBC Traps.....	40

4 Database Tasks.....	51
Backup Command Options.....	51
Backup the Database on a Shutdown Server.....	51
Shut Down the System.....	51
Backup the Database on the Shutdown Server.....	52
Backup the Database on a Running Server.....	52
Restore the Database.....	53
Backup or Restore Reporting Services for Report Manager.....	54
5 High Availability.....	55
Overview.....	55
Session Delivery Manager HA Cluster.....	55
Terminology.....	55
HA Process.....	56
Co-location.....	57
Single Master with Multiple Replica Strategy.....	57
Multi-Member Clustering.....	57
Two-Member Clustering.....	60
Data Synchronization Scenarios.....	63
Add a Member to an Existing Cluster.....	63
Member of a Cluster Fails or is Shutdown.....	63
Member Rejoining a Cluster.....	63
High Availability Scenarios.....	64
Retire a Cluster Member.....	64
Network Partition in Two Node Cluster.....	65
Network Partition in a Three Node Cluster.....	65
A— Available Session Delivery Manager Server Scripts.....	67

About This Guide

This document and other product-related documents are described in the Related Documentation table.

Related Documentation

Table 1: Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Release Notes	Contains information about the administration and software configuration of the Oracle Communications Session Delivery Manager feature support new to this release.
Installation Guide	The Installation guide describes the process to install the Session Delivery Manager including both the typical installation process as well as the custom installation options.
Administration Guide	Contains information about security administration, which lets you create new users and new user groups, and set group-based authorization.
Security Guide	Provides the following security guidelines and topics: <ul style="list-style-type: none">• Guidelines for performing a secure installation of Oracle Communications Session Delivery Manager on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines.• An overview of the Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system.• Security maintenance, which includes a checklist to securely deploy Oracle Communications Session Delivery Manager on your network, maintaining security updates, and security considerations for developers.

Table 2: Oracle Communications Session Element Manager Documentation Library

Document Name	Document Description
User Guide	Contains detailed information pertaining to the Session Element Manager application and describes the dashboard summary view, audit log, fault, and performance views.

About This Guide

Document Name	Document Description
Web Services SOAP XML Provisioning API Guide	Contains a full description of the individual interface definitions that make up the Application Programming Interface (API).

Table 3: Oracle Communications Report Manager Documentation Library

Document Name	Description
User Guide	Contains information about configuring Report Manager to interoperate with Oracle BI Publisher as well as creating reports on network devices.
Installation Guide	Contains instructions for installing Oracle Communications Report Manager as an Add-on to the Session Delivery Manager including the database and BI Publisher components.

Table 4: Oracle Communications Session Route Manager Documentation Library

Document Name	Description
User Guide	Contains documentation and about using the Session Route Manager with Oracle Communications Session Delivery Products.

Revision History

Date	Description
August 2015	<ul style="list-style-type: none">Initial ReleaseUpdates were made to the product name.
April 2016	<ul style="list-style-type: none">The Oracle Legal Notices section was updated.Hierarchical service configuration (HSC) folder permissions were added to the Security Manager chapter.The <i>Configure External User Authentication</i> section and subsections were updated in the Security Manager chapter.The <i>Add and Map a Local User Group to an External Domain User Group</i> section was added to the Security Manager chapter.
May 2016	<ul style="list-style-type: none">The Backing-up and Restoring the Database chapter was renamed Database Tasks.In the Database Tasks chapter, the <i>Restore the Database</i> section replaces the <i>Restoring the Database Backup with Server Shutdown</i> and <i>Restoring the Database While the Server is Running</i> sections. The <i>Backing-Up Database Servers</i> section

Date	Description
	<p>was renamed <i>Backup Command Options</i>. Other sections were renamed and improved.</p> <ul style="list-style-type: none">• Updated the <i>Configure Device Clusters</i> section in the High Availability chapter. New sub-sections were added and existing sub-sections were improved and reorganized.
June 2016	<ul style="list-style-type: none">• The <i>Configure Device Clusters</i> section in the <i>High Availability</i> chapter moved to the <i>Device Manager</i> chapter of the <i>Oracle Communications Session Element Manager User Guide</i>.
July 2016	<ul style="list-style-type: none">• Added the <i>Available Session Delivery Manager Server Scripts</i> appendix.

Health Monitor

Overview

If you have Administration privileges you can access the Health Monitor console to detect certain types of issues before they can compromise Oracle Communications Session Delivery Manager applications. The Health Monitor provides the administrator with the tools to pro-actively address potential problems in Oracle Communications Session Delivery Manager.

The Health Monitor provides heartbeat indicators and statistics related to Oracle Communications Session Delivery Manager server status and disk utilization for servers configured as members of a Oracle Communications Session Delivery Manager cluster. The Health Monitor displays:

- heartbeat status information and statistics related to members of a Oracle Communications Session Delivery Manager server cluster
- server inactive and active count
- disk usage and directory statistics


The Health Monitor includes the Heartbeat Monitor, which detects heartbeat messages and reports on server status and the Disk Usage Monitor, which provides information about disk usage and the size of several Oracle Communications Session Delivery Manager directories.


Accessing the Health Monitor Console

To access the Health Monitor Console:

From the Oracle Communications Session Delivery Manager Tools menu, choose Health Monitor. The Health Monitor Console appears in the Content area.

Health Monitor Console

Select Monitor: 

Select Source: 

Heartbeat Summary

Cluster Member	Status	Up Time (dd:hh:mm)	Down Time (dd:hh:mm)	Last Heartbeat Timestamp	Heartbeat Count	Missed Heartbeat Count	HBFM	MHFM	Inactivity Count	Reset Count
172.30.10.136 (Master)	ACTIVE	02:23:01	NA	2011-05-16 13:10:24	942	0	0	1	0	0
172.30.80.19	ACTIVE	00:02:37	NA	2011-05-16 14:11:53	940	0	0	1	0	0
172.30.10.131	ACTIVE	00:01:18	NA	2011-05-16 13:10:22	942	0	0	1	0	0

The Heartbeat Monitor display appears by default. From here you can choose to display the statistics for the different members of the cluster or you can choose to access the Disk Usage monitor.

Heartbeat Monitor

The Heartbeat Monitor maintains the statistics of Oracle Communications Session Delivery Manager server heartbeats for all members in a cluster. It also keeps a count of the times a member was considered inactive and the number of times it returned to an active state based on the number of received and missed heartbeats, and a set threshold.

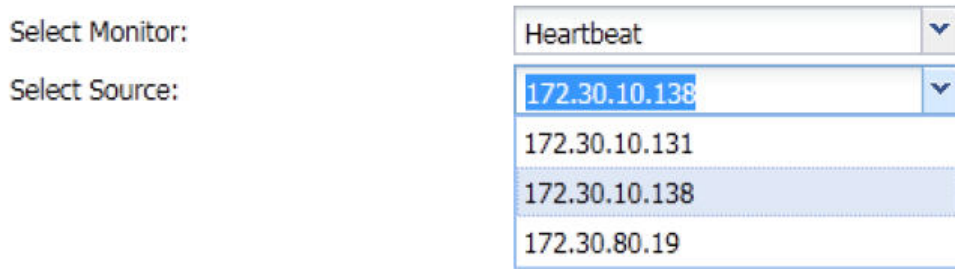
To view heartbeat statistics:

1. In the Health Monitor Console display, ensure Heartbeat is selected in the Select Monitor drop-down list.

By default the IP address displayed in Select Source is for the server on which Oracle Communications Session Delivery Manager is running and servicing the current client session.

2. Click the down arrow for Select Source to choose from a list of server IP addresses for the other cluster members or retain the default value.

Health Monitor Console



The Heartbeat Summary table displays the cluster gathered statistics as maintained by the selected server. Each server maintains their own separate statistics of each server in the cluster. In the case of failure of one member of the cluster, all other active members can still relate the last known statistical health of the server before it failed.

Heartbeat Summary											
Cluster Member	Status	Up Time (dd:hh:mm)	Down Time (dd:hh:mm)	Last Heartbeat Timestar	Heartbeat Count	Missed Heartbeat Count	HBFM	MHFM	Inactivity Count	Reset Count	
172.30.10.138 (Master)	ACTIVE	02:23:42	NA	2011-05-16 13:51:02	43636	0	0	0	1	1	
172.30.80.19	ACTIVE	00:03:17	NA	2011-05-16 14:52:33	265	0	0	0	16	16	
172.30.10.131	ACTIVE	00:01:59	NA	2011-05-16 13:51:00	1426	0	0	0	2	2	

The following table list the statistics tracked along with a description.

Statistic	Description
Cluster Member	IP address of the host member of the Oracle Communications Session Delivery Manager cluster. If the host IP address has the (Master) label appended, it means this host member is running the master replication database.
Status	Current status of the host member of the cluster. A status of ACTIVE means the member is actively participating in the Oracle Communications Session Delivery Manager cluster. A status of DOWN means this host member has failed to send its heartbeats and is considered as either having failed or a network partition exists between the cluster and this member.
Up Time (dd:hh:mm)	Number of days, hours and minutes the Oracle Communications Session Delivery Manager server has been up
Down Time (dd:hh:mm)	Number of days, hours and minutes the Oracle Communications Session Delivery Manager server has been down

Statistic	Description
Last Heartbeat Timestamp	Date and time of the last known heartbeat for each host member as recorded by the Select member statistics being viewed.
Heartbeat Count	Total count of Oracle Communications Session Delivery Manager server heartbeats
Missed Heartbeat Count	Total number of times the monitor on the targeted host member (Selected Source) missed a heartbeat from other members in the cluster. An increase in this statistic might indicate network issues between members in the Oracle Communications Session Delivery Manager cluster.
HBFM	Heartbeat Failure Meter statistic indicates the amount of times the required heartbeat counter of a Oracle Communications Session Delivery Manager member was not received by the target host member. This number increases when the heartbeats start arriving again. If this statistic reaches a count of 10 (default) this host member is considered by the target host member to be down and its status is set to DOWN.
MHFM	Maximum Heartbeat Failed Meter statistic maintains the high-water mark of the HBFM statistic. This statistic is only reset if a member that left the cluster (status=DOWN) rejoins and starts sending heartbeats again.
Inactivity Count	Number of times the host member was considered to be in the state DOWN by the targeted (Selected Source) member.
Reset Count	Number of times the targeted member (Selected Source) has determined that a host member has gone from a state of DOWN to a state of ACTIVE. If a member rejoins the cluster after being DOWN, the reset counter is incremented by 1 and MHFM is reset to 0.

From here you can choose one of the other members of the cluster from the Select Source drop-down list of choose to view disk usage information.

Disk Usage

The Disk Usage Monitor maintains the statistics on disk storage usage, and checks if disk usage exceeds two threshold levels, 50% and 90% disk full. The Disk Usage monitor inspects the disk usage for the selected system and gathers statistics for total disk storage, used disk capacity, and free disk capacity. It also provides information about the size of the Oracle Communications Session Delivery Manager directories and indicates the partition on which the directory is located. For example, the database directory might be located on a different partition from the other two directories.

Summary

To view summary statistics:

1. Select Disk Usage from the Select Monitor drop-down list.

Health Monitor Console

Select Monitor:

Select Source:

Health Monitor

- Click the down arrow for Select Source to choose from a list of server IP addresses for the members of the cluster or retain the default value.

Health Monitor Console


Select Monitor:

Select Source:

- 172.30.10.131
- 172.30.10.138
- 172.30.80.19

The Disk Usage Summary view appears.

Summary		Details
Cluster Member	peryton	
Path	/apps/AcmePacket/NNC700B83	
Status	NORMAL	
Capacity	216.68 GB	
System Used Space	2.25 GB	
Free Space	214.43 GB	
Percent Usage	1.04 %	

-  **Note:** The summary tab shows the statistics for the partition that Oracle Communications Session Delivery Manager is installed on. If some parts of Oracle Communications Session Delivery Manager, for example, the database, are installed on different partitions, the summary tab will display a table with the statistics of the different partitions.

The following table lists the disk summary statistics along with a description.

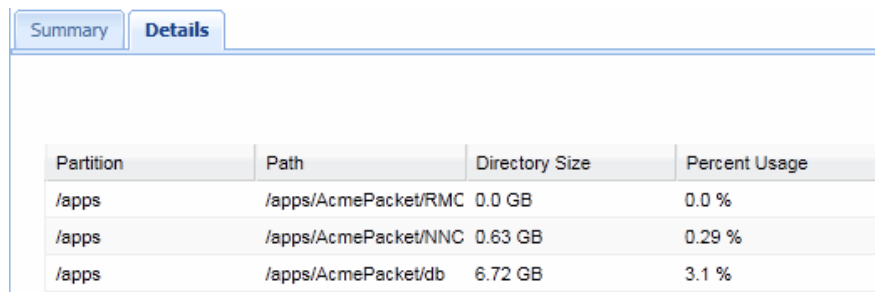
Statistic	Description
Cluster member	Name of the Oracle Communications Session Delivery Manager server
Path	Path to where Oracle Communications Session Delivery Manager is installed.
Status	Status of partition space use: Normal: below the minimum threshold value (default is 50%) Warning: at or above the minimum threshold value but below the maximum threshold value (default is 90%) Critical: at or above the maximum threshold value (default is 90%)
Capacity	Total partition disk space in GB.
System Used Space	Total amount of disk space being used.
Free Space	Remaining disk space in GB.
Percent Usage	Percent of used space for the entire partition.

Details

The Details tab displays information about the space being taken up by the Oracle Communications Session Delivery Manager directories: Oracle Communications Session Delivery Manager, RMCArchive, and DB. It also shows the size of each directory and the percentage of space taken up by each directory.

To access details:

Click the Details tab. The Details table appears.



Partition	Path	Directory Size	Percent Usage
/apps	/apps/AcmePacket/RMC	0.0 GB	0.0 %
/apps	/apps/AcmePacket/NNC	0.63 GB	0.29 %
/apps	/apps/AcmePacket/db	6.72 GB	3.1 %

There are three directories listed in the example that are all located on the same partition.

The following table lists the information included in the Details view.

Statistic	Description
Partition	Name of the partition where the directory is located
Path	Path indicating the location of the directory
Directory Size	Amount of disk space used in the directory in GB
Percent Usage	Percentage of partition space being used by the specific directory

Security Manager

The Security Manager product allows a user with administrator privileges to do the following:

- Create and manage users.
- Create and manage groups.
- Configure security authorization levels, policies and privileges for user groups.
- Provide specific access controls for individual user groups, views, and operations.
- Limit access to specific features and functionality for specific users.
- Configure audit log parameters.

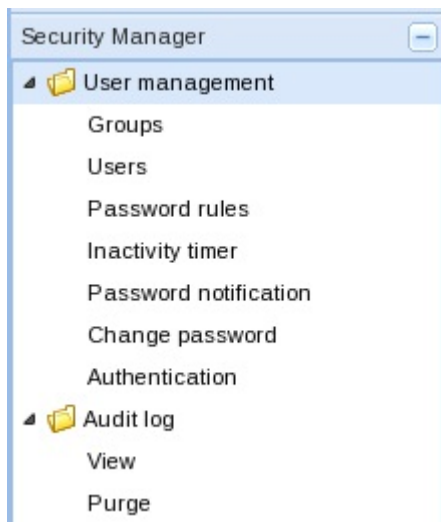


Figure 1: Security Manager Slider Parameters

Configure External User Authentication


Users belonging to the external domain user group are authenticated outside of Oracle Communications Session Delivery Manager by an external domain server. You can select either a RADIUS domain server or Active Directory (AD) domain controller:

- A RADIUS server provides centralized Authentication, Authorization, and Auditing/Accounting (AAA) security protocol management for users who connect and use a network service.

Security Manager

- An AD domain controller provides a directory service in a Windows domain type network using Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

An external domain user group must be mapped to an internal (local) user group in Oracle Communications Session Delivery Manager so that this external domain user group and its users inherit the authorization privileges that are specific to the local user group. See the *Add and Map a Local User Group to an External Domain User Group* section of this chapter for more information.


 **Note:** Internal and external users are both supported simultaneously. However, external users do not have corresponding stored user records or username and password information.

Configure a RADIUS Server

This task is used to configure a RADIUS server domain for external user authentication.

- The RADIUS server must be configured to use the same shared secret string for all cluster nodes.
 - The RADIUS server must be configured to return one or more attribute values in the authentication response message to represent the groups to which a user belongs.
1. Expand the **Security Manager** slider and select **User Management > Authentication**.
 2. In the **External authentication** pane, select the **RADIUS** radio button and click **Add**. The **RADIUS** servers table becomes available for use.
 3. In the **Add a radius server** pane, complete the following fields:

Name	Description
Address field	The IP address or DNS name of the RADIUS server.
Port field	This field is pre-populated with the default RADIUS server listening port 1812 . If you are using a different listening port on your RADIUS server, enter a new value.
Shared secret field	Click Edit next to the field. In the Encrypted shared secret dialog box, enter the following parameters: <ul style="list-style-type: none">• Shared secret—The string assigned within the RADIUS server configuration to a given RADIUS client.• Confirmed shared secret—The same shared secret string again to confirm your input.
Password authentication mechanism drop-down list	<p>PAP is chosen by default. The password authentication protocol (PAP) is an authentication protocol that uses a password in a point-to-point (PPP) session to validate users before allowing them to access server resources.</p> <p>Choose from the following options if you want to authenticate the user with another protocol:</p> <ul style="list-style-type: none">• CHAP—The challenge-handshake authentication protocol (CHAP) authenticates a user or network host to an authentication entity to protect against replay attacks by the peer through the use of an incrementally changing identifier and a variable challenge value.• MSCHAPV1—The Microsoft CHAP Version 1 (MS-CHAP v1) version of CHAP is used with RADIUS servers to authenticate wireless networks. In comparison with CHAP, MS-CHAPv1 is enabled by negotiating CHAP Algorithm 0x80 in the link control (authentication) protocol (LCP) option 3. LCP option 3 sends the Configure-Nack LCP packet type when all the LCP options are

Name	Description
	<p>recognized, but the values of some options are not acceptable. Configure-Nack includes the offending options and their acceptable values). MS-CHAPv1 also provides an authenticator-controlled password change and authentication retry mechanisms, and defines failure codes, which are returned in the Failure packet message field.</p> <ul style="list-style-type: none"> • MSCHAPV2—The Microsoft CHAP Version 2 (MS-CHAPv2) uses the same authentication as MS-CHAPv1, except that CHAP Algorithm 0x81 is used instead of the CHAP Algorithm 0x80. • EAPMD5—The extensible authentication protocol (EAP-MD5) offers minimal security and is used in wireless networks and point-to-point networks. EAP-MD5 enables a RADIUS server to authenticate a connection request by verifying an MD5 hash of a user password. The server sends the client a random challenge value, and the client proves its identity by hashing the challenge and its password with the MD5 hash. • EAPMSCHAPV2—The protected extensible authentication protocol challenge-handshake authentication protocol (EAP-MSCHAPv2) allows authentication to databases that support the MS-CHAPv2 format, including Microsoft NT and Microsoft Active Directory.
Group attribute name field	<p>This field is pre-populated with the attribute Filter-Id by default.</p> <p> Note: Change the default value if the RADIUS server's group attribute does not match.</p> <p>This attribute (RADIUS attribute 11) is necessary for the device to assign a user to a RADIUS group. This RADIUS attribute connects the user name with the attribute in order to place this user in a RADIUS group. The group attribute name is configured to be included in Access-Accept message that the RADIUS server returns to this device.</p>

4. Click **Apply**.

External users can now be authenticated by the RADIUS server. See the *Map a Local User Group to an External Domain User Group* section of this chapter for more information.

Configure an Active Directory Domain Controller

This task is used to configure and active directory (AD) domain controller (domain server) for external user authentication.

- The Active Directory must be configured for LDAP over SSL if the Active Directory is enabled in Oracle Communications Session Delivery Manager.
 - Active Directory must support version 5, if the Kerberos protocol is used.
 - Each user object in your Active Directory must store the groups of each member using the *memberOf* attribute.
 - Only child groups may be mapped to local groups when group nesting is in use. This limitation is due to the *memberOf* attribute not containing a recursive list of predecessors when nesting.
1. Expand the **Security Manager** slider and select **User Management > Authentication**.
 2. In the **External authentication** pane, select the **Active directory** radio button and click **Add**. The **Active Directory** servers table becomes available for use.
 3. In the **Add a Domain Controller** pane, complete the following fields:

Security Manager

Name	Description
Address field	The IP address or DNS name of the domain controller.
Domain field	The domain name for the domain controller.
LDAP Port field	The listening port number of the LDAP service. The default is 389. Use port 636 if using SSL.
Password security drop-down list	Select from the following protocols used to authenticate the user: <ul style="list-style-type: none">• Digest-MD5—The password cipher based on RFC 2831.• LDAP over SSL—The SSL to encrypt all LDAP traffic.• Kerberos—The Kerberos protocol to authenticate the user by specifying an existing krb5.conf file containing the information needed by the Kerberos V5 library. This includes information describing the default Kerberos realm, and the location of the Kerberos key distribution centers for known realms.

4. Click **Apply**.

External users can now be authenticated by the AD domain controller. See the *Map a Local User Group to an External Domain User Group* section of this chapter for more information.

Configure Groups

You can configure a local group to be mapped to an external domain user group so that the external group can inherit the authorization privileges of this local group. You can also add and manage additional local groups other than the default local groups that are provided by Oracle Communications Session Delivery Manager.

Find an External Domain User Group

Use the external membership tool to find the name of an external domain user group so that it can be later mapped to a local (internal) user group.

This tool provides the ability to test external users once an external domain server is configured and returns a list of external domain user groups to which the external domain user was assigned. This makes finding the proper external domain user group names that you need to map to the local user group easier so that the external domain user group can inherit its authorization privileges. Once you find the external domain user group you want, see the *Add and Map a Local User Group to an External Domain User Group* section of this chapter to continue.

1. Expand the **Security Manager** slider and select **User Management > Groups**.
2. In the **User Groups** pane, select the local group name that you are using for the external RADIUS user group (for example, MyExternalRADIUSUserGroup) and click **Edit**.
3. In the **Configuration** tab, enter the external group name (for example, Domain Users) and click **Apply and Test**.

The **Test group membership** dialog box displays with results for the external group.

Test group membership

Group name: Domain Users

User name: user12

Password: Edit

Address: lab-dc01.acmepacket.com

Results

Domain controller group names
BDL[vm domain]{a24a6ac5-d1cc-4de7-923...
CSeriesDeliveries
DSeriesDeliveries
Domain Users
EMS6SeriesDeliveries
EMSTSeriesDeliveries
EMSTSeriesSpecReviewers
EMS_Bugs
EMS_Dev
ESeriesDeliveries
Engineering
Management Systems
ManagementApps
NetworkMgmt
Project-Eng
SP Data Services

Test Cancel

Figure 2: Example of Test Group membership results for an external group:

Add and Map a Local User Group to an External Domain User Group


Use this task to allow the external domain user belonging to the external domain user group to inherit the group-based authorization privileges of the local user group.

The external domain user is authenticated by a domain server, such as a RADIUS server or Active Directory domain controller. You must map the external domain user group to the local (internal) user group that was created for this purpose.

See the *Use the External Membership Tool to Find External Domain User Groups* section of this chapter for more information about finding the external domain user group name that you need for this task.

1. Under the **User Management** folder, select the **Groups** leaf node.
2. In the **User Groups** pane, click **Add**.
3. In the **Add Group** dialog box, complete the following fields:

Security Manager

Name	Description
Group name field	<p>The local user group name that you want to use for authorization privileges. For example, LocalUGforDomainUG. Use the following guidelines for naming this group:</p> <ul style="list-style-type: none"> • Use a minimum of three characters and maximum of 50. • The name must start with an alphabetical character. • You are allowed to use alphanumeric characters, hyphens, and underscores. • The user group name is case insensitive. • The user group must be unique.
External group name field	<p>For Active Directory (LDAP), the external domain user group name. For example, Domain UG.</p> <p>For RADIUS, the external group name should map to attribute 11 (Filter-ID), which is in the RADIUS reply.</p> <p> Note: You must have at least one external domain user group entry configured on the domain server in order for this field to be displayed in the dialog box.</p>
Group permissions copy from drop-down list	<p>Choose from the following default user groups to copy their privileges:</p> <ul style="list-style-type: none"> • None—Manually configure privileges for this user group. • administrators—This super user group is privileged to perform all operations. • LIAdministrators—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • provisioners—This group is privileged to configure Oracle Communications Session Delivery Manager and save and apply the configuration with the exception of a LI configuration. • monitors—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Session Delivery Manager, and has the fewest privileges.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. Log out and log back into the system with the external RADIUS user to test your external connection to Oracle Communications Session Delivery Manager.

Add a Local User Group

A local (internal) user group is a logical collection of users grouped together to access common information or perform similar tasks in Oracle Communications Session Delivery Manager. You assign specific authorization privileges to a group and then assign users to it. Those users in turn, inherit the group-based privileges. See the *Add and Map a Local User Group to an External Domain User Group* section of this chapter if you need to add local group that needs to be mapped to an external domain user group.

1. Expand the **Security Manager** slider and choose **User management > Groups**.
2. In the **User Groups** pane, click **Add** to add a new user group.

3. In the **Add Group** dialog box, complete the following fields:

Name	Description
Group name field	<p>The user group name. Use the following guidelines for naming this group:</p> <ul style="list-style-type: none"> • Use a minimum of three characters and maximum of 50. • The name must start with an alphabetical character. • You are allowed to use alphanumeric characters, hyphens, and underscores. • The user group name is case insensitive. • The user group must be unique.
Group permissions copy from drop-down list	<p>Choose from the following default user groups to copy their privileges:</p> <ul style="list-style-type: none"> • None—Manually configure privileges for this user group. • administrators—This super user group is privileged to perform all operations. • LIAdministrators—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • provisioners—This group is privileged to configure Oracle Communications Session Delivery Manager and save and apply the configuration with the exception of a LI configuration. • monitors—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Session Delivery Manager, and has the fewest privileges.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. Click **Back** to return to the **User Groups** table.

Delete a User Group

1. Expand the **Security Manager** slider and choose **User management > Groups**.
2. In the **Groups** pane, choose the (non-default) user group that you want to delete from the **User Groups** table and click **Delete**.
3. In the **Delete** confirmation dialog box, click **Yes** to delete this user group. The user group is removed from the **User Groups** table.
4. In the success dialog box, click **OK**.

Change Privileges for User Groups

By default, privileges are assigned to each category of a user group that allow or deny all users within this user group the ability to perform certain operations. You have the option to change the default privilege type for items in each category item of a pre-existing user group or a user group that you create allow or deny all users within this group the ability to perform certain operations. This includes items intended for use with separate application products that you are licensed to use.

Operations Tree Structure

The operations tree structure contains all the security configuration and administrative tasks you can perform in Oracle Communications Session Delivery Manager. It is logically arranged with parent and child operations that can be accessed once user group and user accounts are created. Individual access to a specific operation within the tree structure can be provided or denied by assigning a privilege to it. Although Oracle Communications Session Delivery Manager displays all the operations it supports, some apply only to users who are licensed for a specific application operation.

The top of the operations tree is the root. There can be one or more operation categories below the root that serve as parents for individual operations (children). The child privilege type of higher-level (or parent) operation is equal or less than the privilege type of its parent. When you change the privilege type of a parent, the child privilege type can change based on this rule. However, if the parent privilege type is returned to its previous privilege type, the child remains at the privilege type to which it was bumped and needs to be promoted manually.

Apply User Group Privileges for the Administrative Operations

1. Expand the **Security Manager** slider and choose **User management > Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. In the expanded group pane, click the **Administrative operations** tab and click the folder and subfolder sliders to expand the item operations list.
4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following user group privilege options for folders or items in the **Administrative operations** tab table described below:
 - **Full**—(Default) Allowed to perform administrative operations.
 - **None**—Not allowed to perform administrative operations.
 - **View**—Allowed to monitor only.

Name	Description
Administrative operations folder	Set privilege levels for all of the following administrative operations.
Security administration folder	Set privilege levels for all of the following user management operations accessible on the Security Manager slider.
Group operations folder	Set privilege levels for all group item operations.
Add group item	Add a new group.
Update group item	Modify groups.
Delete group item	Delete existing groups.
User operations folder	Set privilege levels for all the following user operations accessible on the Security Manager slider.
Add users item	Create new users.
Update users item	Modify user information.
Delete users folder	Delete existing users.
Reset password item	Reset your password used to login <i>Oracle Communications Report Manager</i> to <i>Oracle Communications Report Manager</i> .

Name	Description
Change password item	Change another user's password used to login to <i>Oracle Communications Report Manager</i> .
Change inactivity timer item	Change the inactivity timer, which logs off the user if the client is no longer being used.
Change Password Rule item	Configure the password rules used when creating a new user.
Edit login banner	Edit the login banner for users logging into <i>Oracle Communications Report Manager</i> .
Password notification	Change the notification interval.
Device group folder	Assign privilege to all of the following device group operations accessible through the Device Manager slider
Add device group item	Add a new device group.
Delete device group item	Delete a device group.
Move device group item	Move a device group.
Rename device group item	Rename a device group.
Device folder	Assign privilege to all of the following device operations accessible through the Device Manager slider.
Activate device	Activate a new device.
Add device item	Add a new device.
Remove device item	Remove an existing device.
Move device item	Move a device.
KPI Operation item	Set privilege levels to get device KPIs, register KPIs, deregister KPIs, or update registered KPIs.
Edit login banner item	Allow users of a group to change the informational banner seen when a user logs into <i>Oracle Communications Session Delivery Manager</i> .
Change password message interval item	Send alert that prompts user to change their password a certain number of days before their password expires.
View all audit logs item	View all audit logs.
View own audit log item	View only personal audit log.
Change audit log auto purge interval item	Configure the number of days of audit logs to keep.
Export audit logs item	Export all or part of an audit log to a file.
Manual audit log purge item	Manually purge audit logs.
View health monitor console item	Access health monitor console to detect issues.
Change configuration archive settings item	Change configuration archive settings.
Update OS/System account password item	Update the operating system and the system account password.

Security Manager

Name	Description
Authentication item	Update authentication parameters.
Server Diagnostics item	Access to server diagnostics.

6. Click **Apply**.

Apply User Group Privileges for Fault Management Operations

An element manager system (EMS) must be licensed to apply user-group privileges for fault management operations that apply to the events and alarms that appear on the **Fault Manager** slider.

1. Expand the **Security Manager** slider and choose **User management > Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. Click the **Fault management** tab and click the folder and subfolder sliders to expand the item operations list.
4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following user group privilege options for folders or items in the **Fault management** tab table described below:
 - **Full**—(Default) Allowed to perform event or alarm operations.
 - **None**—Not allowed to perform event or alarm operations.

Name	Description
Fault management folder	If the None privilege is chosen, the Fault Manager slider does not appear in the Oracle Communications Session Delivery Manager GUI.
Events and Alarms folder	Assign the privileges for all of the following event and alarm operations accessible on the Fault Manager slider.
Alarms folder	Assign the privileges for all of the following alarm operations accessible on the Fault Manager slider.
Set email notification item	Create an email list for alarms.
Delete alarm item	Delete alarms.
Remap severities item	Edit the alarm severity levels.
Events folder	Assign the privileges for all of the following event operations accessible on the Fault Manager slider.
Delete events item	Delete events.
Configure trap receiver item	Assign privileges to configure a trap receiver.

6. Click **Apply**.

Apply User Group Privileges for Applications

1. Expand the **Security Manager** slider and choose **User Management > Groups**.
2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.
3. Select the **Applications** tab and click to expand the **Applications** folder.
4. Select any folder or folder item row that are described in the table below that you want to modify and click the **Privileges** column to activate the drop-down list.

Select the following privilege from the **Privileges** drop-down list:

- **Full**—Enable GUI elements (such as tabs) to perform configuration operations.
- **View**—View information only.
- **None**—Disable configuration operations and make them disappear from the GUI.

Name	Description
Application folder	Set privilege levels for all of the following applications operations.
Report Manager folder	Set privilege levels for all reporting operations accessible on the Report Manager slider.
Execute Reports item	Set privilege levels for users belonging to a group to run reports. If given full privileges, collection reports can be configured.
Administration folder	Set all administration privileges for <i>Oracle Communications Report Manager</i> .
Configure Retention Policy item	Set privilege levels for a user group to create a retention policy for retaining Historical Data Recording (HDR) data over a period of time.
Register BI Publisher item	Set privilege levels for the <i>Oracle Communications Report Manager</i> to register with the <i>Oracle Communications Session Delivery Manager</i> before creating and running reports.

5. Click **Apply**.

Apply User Group Privileges for Product Configurations

You can apply user-group privileges in the Oracle Communications Session Delivery Manager to enable certain product configuration operations.

1. On the navigation bar, select **Security Manager > User management > Groups**.
2. In the **User Groups** pane, select the group you want to modify from the **User Groups** table and click **Edit**.
3. Select the **Configuration** tab and click to expand the **Configuration** folder.
4. Select any folder or folder item row that are described in the table below that you want to modify and click the **Privileges** column to activate the drop-down list.

Select the following privilege from the **Privileges** drop-down list:

- **Full**—Enable GUI elements (such as tabs) to perform configuration operations.
- **View**—View information only.
- **None**—Disable configuration operations and make them disappear from the GUI.

Name	Description
SBC configuration folder	Choose the permission level for all configuration operations. If you choose None , the Configuration Manager and Route Manager sliders are prevented from appearing in the <i>Oracle Communications Session Element Manager</i> or <i>Oracle Communications Session Route Manager</i> GUIs.
Configure services item	Configure the signaling services for a <i>Oracle Communications Session Border Controller</i> . Includes SIP, DNS ALG, H.323, MGC{P, H248
Configure interfaces item	Configure a physical and network interfaces for a <i>Oracle Communications Session Border Controller</i> .
Configure NM controls item	Configure network management controls for multimedia traffic.

Security Manager

Name	Description
Configure security item	Configure the following <i>Oracle Communications Session Border Controller</i> security features: <ul style="list-style-type: none"> • Transport Layer Security (TLS) • Internet Protocol Security (IPsec) • RADIUS accounting and server authentication • Packet tracing • Password policy
Configure LI item	Configure lawful intercept for the <i>Oracle Communications Session Border Controller</i> if licensed.
Configure system item	Configure <i>Oracle Communications Session Border Controller</i> system.
Route Management Central configuration folder	Enables <i>Oracle Communications Session Route Manager</i> if it is licensed.
Configure route set item	Configures route set actions for updating devices.
Configure templates item	Configure the templates used for mapping the columns of the CSV files to the properties of the routes, allowing for the import of CSV files.
Backup/Restore item	Create backup files of the route set(s) and restore the backup files to the device.
Device operation item	Add route sets to devices, view the route sets associated with each device, update route sets, and update task histories.
Work order folder	Allow user to upgrade and manage <i>Oracle Communications Session Border Controller</i> devices.
Create work order item	Allow user to create <i>Oracle Communications Session Border Controller</i> device upgrade operations.
Execute work order item	Allow user to execute <i>Oracle Communications Session Border Controller</i> device upgrade operations.
Load device item	Allow user to load and manage <i>Oracle Communications Session Border Controller</i> devices.
Override lock	Override a lock set by user on a managed device configuration.
Transfer configuration view item	Transfer ownership of records in the local configuration view.
Entitlements item	Get the licensed-based entitlements for features enabled on the device.
Apply to SBC folder	Save, activate, and activate saved <i>Oracle Communications Session Border Controller</i> configuration edits.
Save configuration item	Save the <i>Oracle Communications Session Border Controller</i> configuration edits made using Oracle Communications Session Delivery Manager.
Save and activate configuration item	Save and activate <i>Oracle Communications Session Border Controller</i> configuration edits made using Oracle Communications Session Delivery Manager.
Activate configuration item	Activate saved <i>Oracle Communications Session Border Controller</i> configuration edits made using Oracle Communications Session Delivery Manager.

Name	Description
Configuration archive folder	Allow user to manage the configuration archive for <i>Oracle Communications Session Border Controller</i> devices.
Back up configurations item	Allow user to back up configurations in the archive for <i>Oracle Communications Session Border Controller</i> devices.
Restore configurations item	Allow user to restore configurations in the archive for <i>Oracle Communications Session Border Controller</i> devices.
Delete archived configurations	Allow user to delete configurations in the archive for <i>Oracle Communications Session Border Controller</i> devices.

5. Click **Apply**.

Apply User Group Privileges for Session Border Controller System Boot Parameters

1. On the Oracle Communications Session Delivery Manager navigation bar, choose **Security Manager > User management > Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. Click the **SBC system maintenance** tab for which you want to modify privileges and click on the folder slider to expand the item operations list.
4. Choose the item row in the operation category table that you want to modify and click the **Privileges** column to activate the drop-down list.
5. In the **Privileges** drop-down list, choose the following options:
 - **Full**—The user group is allowed to reboot the *Oracle Communications Session Border Controller*.
 - **None**—The user group is not allowed to reboot the *Oracle Communications Session Border Controller*.
6. Click **Apply**.

Apply User Group Privileges for Device Groups

Use this task to apply user-group privileges for device groups that appear on the **Device Manager** slider.

1. On the Oracle Communications Session Delivery Manager navigation bar, choose **Security Manager > User Management > Groups**.
2. In the **User Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
3. Click the **Device group instances** tab.
4. In the **Device groups** box table, complete the following fields:

Name	Description
Include children check box	Check the check box to include the choice of preference for all children of this device group.
Home item	(Default device group) In the Privileges column drop-down list, choose the following user group privilege options for items in the Device groups box table described below: <ul style="list-style-type: none"> • Full—(Default) Allowed to perform event or alarm operations. • None—Users do not have authorization to the device group. • View—Users can view the group on the Device Manager slider, but cannot perform any operations such as adding or deleting a child group.

Security Manager

The **Preview** box displays the device group based on the privileges that are assigned (**Full, View**).

5. Repeat the previous step for other device groups (if there are any).
6. Click **Apply**.

Configure Users

A user is a person who logs into the system to perform application-related operations. Before this user can access any operations, they must be added to a user group. Each user group has a defined set of privileges. The operations that a user can do depends on the privileges of the user group to which the user belongs.

The following users are created by default when Oracle Communications Session Delivery Manager is installed:



- **admin**—Inherits the privileges from the **administrators** group.
- **LIadmin**—Inherits the privileges from the **LIadmin** group.

Users (other than the default users) are created, added, and given the privileges of the user groups to which they are assigned so that they can access Oracle Communications Session Delivery Manager.

Add a User

1. Expand the **Security Manager** slider and choose **User Management > Users**.
2. In the **Users** pane, click **Add**.
3. In the **Add User** dialog box, complete the following fields:

Name	Description
Group Assigned group drop-down list	Choose from the following default user groups: <ul style="list-style-type: none">• administrators—This super user group privileged to perform all operations.• LIAdministrators—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups.• provisioners—This group is privileged to configure Oracle Communications Session Delivery Manager and save and apply the configuration with the exception of a LI configuration.• monitors—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Session Delivery Manager, and has the fewest privileges.
User information User name field	The name of the user using the following guidelines: <ul style="list-style-type: none">• Use a minimum of 3 characters and maximum of 50 characters.• The name must start with an alphabetical character.• The use of alphanumeric characters, hyphens, and underscores are allowed.• The name is case insensitive.• The name cannot be the same as an existing group name.

Name	Description
User information Password field	The password is entered for this user using the following guidelines: <ul style="list-style-type: none"> • The password must be at least 8 characters long. • Use at least one numeric character from 0 to 9 in the password. • Use at least one alphabetic character from the English language alphabet in the password. • Special characters include { , , } , ~ , [, \ ,] , ^ , _ , ' , : , ; , < , = , > , ? , ! , " , # , \$, % , & , ` , (,) , * , + , , , - , . , and /
User information Confirm password field	The same password entered again to confirm it.
User account expiration dates Account field	Uncheck the check box to change the user account expiration date. Click the calendar icon to open a calendar to choose the date after which the user account expires.  Note: If the check box is checked (default) the user account never expires.
Password expiration dates Password field	Uncheck the check box to change the password expiration date. Click the calendar icon to open a calendar to choose the date after which the user password expires.  Note: If the check box is checked (default) the password never expires.



4. Click **OK**.

The following information displays in the **Users** table:

Name	Description
User name column	The user name.
Group column	The user group to which the user belongs.
Status column	The status of the user account is either enabled or disabled .
Operation status field	The state of the user account and its expiration date: <ul style="list-style-type: none"> • active—The account is valid and the user can log in. Neither the account nor password expiration dates have been exceeded. • account expired—The account expiration date has expired. • password expired—The password expiration date has expired. • password deactivated—The failed login attempts by the user exceeded the allowed number of tries as specified by the value set for password reuse count parameter in password rules. • locked out—The user has exceeded the login failures and the account is disabled until the lockout duration has passed.

Edit a User

1. Expand the **Security Manager** slider and choose **User Management > Users**.
2. In the **Users** pane, choose a user and click **Edit**.
3. In the **User** tab , change the following fields:

Name	Description
Assigned group drop-down list	<p>Change the assigned user group:</p> <ul style="list-style-type: none"> • administrators—This super user group privileged to perform all operations. • LIAdministrators—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups. • provisioners—This group is privileged to configure Oracle Communications Session Delivery Manager and save and apply the configuration with the exception of a LI configuration. • monitors—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Session Delivery Manager, and has the fewest privileges.
User status Administrative status drop-down list	Choose if the user status is either enabled or disabled .
Expiration dates Account field	<p>Uncheck the check box to change the user account expiration date. Click the calendar icon to open a calendar to choose the date after which the user account expires.</p> <p> Note: If the check box is checked (default) the user account never expires.</p>
Expiration dates Password field	<p>Uncheck the check box to change the password expiration date. Click the calendar icon to open a calendar to choose the date after which the user password expires.</p> <p> Note: If the check box is checked (default) the password never expires.</p>

4. Click **Apply**.

Reactivate a User

A user can be denied access to Oracle Communications Session Delivery Manager if the user is disabled, expired, the user password expired, or the user logs in more times (due to failed log in attempts) than is allowed by the Password reuse count value.

You can reactivate a user by editing the user profile to reset the status of the user to enable, then reset the expiration in days for the account and password parameters. You can also delete the expired user and recreate the user.

The following table lists the possible causes for user deactivation and how to reactivate the user.

Cause	Action
User expired	Reset the calendar to a new date.
Password expired	Reset the password calendar to a new date.
Password deactivated	Reactivate the user account by:

Cause	Action
	<ul style="list-style-type: none"> Changing the user password if all expiration dates are still valid. Extending the account expiration date. Extend the password expiration date.
User disabled	Reset the user to enabled.

Delete a User

1. Expand the **Security Manager** slider and choose **User management > Users**.
2. In the **Users** pane, choose a user and click **Delete**.
3. In the **Delete** dialog box, click **Yes**.
4. In the success dialog box, click **OK**.
The user name is removed from the **Users** table.

Reset a User Password

You must have permission to reset passwords.

1. Expand the **Security Manager** slider and select **User management > Users**.
2. In the **Users** pane, click a user from the table and click **Reset Password**.
3. In the **Reset password** dialog box, enter a new password for the user in the field provided.
4. The dialog box indicates if you entered the new password successfully. Click **OK**.

Change a User Password

If you have administrative operations permission, you can change the password of a user.

1. Expand the **Security Manager** slider and select **User Management > Users**.
2. In the **Users** pane, click a user from the table and click **Change Password**.
3. In the **Change password** dialog box, complete the following fields:

Name	Description
Enter your password field	Enter the existing password for the user.
Enter new password for user field	The new password for the user.
Confirm new password for user field	The new password is entered again to confirm it.

4. Click **OK**.


Change User Password Rules

Use this task to change the password rules that specify the length of the password, how many times it can be reused, and whether specific characters, such as a numeric value, can be used.

1. Expand the **Security Manager** slider and select **User management > Password rules**.
2. In the password rules pane, complete the following fields:

Name	Description
Maximum login fail attempts For administrator	The value that indicates the maximum login attempts allowed before the user is locked out of the system. You can set a different value for

Security Manager

Name	Description
users and For non-administrator users fields	both administrator users and non-administrator users. The default value is 5 attempts.
Account lockout duration For administrator users (minutes) field	Enter the number of minutes that an administrator user is locked out after the maximum login fail attempts For administrator users value has been reached. The default is 15 minutes.  Note: This parameter applies to Administrator users only. Non-administrator users remain locked out until their login is reset.
Password reuse count For all users field	The value that indicates the number of counts to use to prevent the reuse of a password. The reuse count restricts the user from reusing the password entered in the last number of counts. For example, if you enter 2 here the user cannot reuse the same password used on the previous two occasions. You can change the password for this user by using the guidelines below.
Password length for administrator users Minimum length and Maximum length fields	The values for the minimum (no less than eight characters) and maximum (up to 16 characters) length of a password for a user who has administrator privileges.
Password length for non-administrator users Minimum length and Maximum length fields	The values for the minimum (no less than eight characters) and maximum (up to 16 characters) length of a password for a user who does not have administrator privileges.
Password contains at least one of the following	Check the checkbox for each of the following rules that you want to enforce: <ul style="list-style-type: none"> • Numeric character—Use at least one numeric character from 0 to 9 in the password. • Alphabetic character—Use at least one alphabetic character from the English language alphabet in the password. • Special character—You can include the following: {, , }, ~, [, \,], ^, _ , ' , : , ; , < , = , > , ? , ! , " , # , \$, % , & , ` , (,) , * , + , , , - , . , and /

3. Click **Apply**.

Notify When to Change the User Password

You can configure when the user is notified to change their password before it expires.


When the user logs into Oracle Communications Session Delivery Manager, the system checks user credentials and the password expiry time for the user. If the password is due to expire, Oracle Communications Session Delivery Manager displays a warning and prompts the user to change their password.

1. Expand the **Security Manager** slider and select **User management > Password notification**.
2. In the **Password expiration notification** panel, enter a value in the **Days prior to password expiration** field.
3. Click **Apply**.

Set the Inactivity Timer to Prevent Unauthorized System Access

We recommend that you set the inactivity timer to prevent unauthorized access to your system as soon as possible.

The inactivity timer logs off the user from the Oracle Communications Session Delivery Manager session when its value is exceeded. The user must re-enter their password to continue. You can set different values for a user with administrative permissions and users who do not have administrative permissions.

 **Note:** The default inactivity timer value for an administrator is set to zero (never expire). You must choose a different value to terminate a user session after a specified time period.


1. Expand the **Security Manager** slider and select **User Management > Inactivity timer**.
2. In the **Session timeout** panel, complete the following fields:

Name	Description
Admin field	(Optional) The number of minutes of inactivity after which the user with administrative permissions is logged off. The range is zero to 65535 minutes. Zero sets the inactivity timer to never expire.
Non-Admin field	The number of minutes of inactivity after which a non-administrative user is logged off. The range is 1 to 65535 minutes. Thirty minutes of user inactivity is the default.

3. Click **Apply**.

Audit Logs

You can use the audit log (containing audit trails) generated by Oracle Communications Session Delivery Manager to view performed operations information, which includes the time these operations were performed, whether they were successful, and who performed them when they were logged into the system.

 **Note:** Audit logs contain different information depending on its implementation.

Audit trails include the following information:

- The user who performed the operation.
- What operation was performed by the user.
- When the operation was performed by the user.
- Whether the operation performed by the user was successful or failed.

View and Save an Audit Logs

The following Oracle Communications Session Delivery Manager operations are logged:

- User logins and logouts.
- Managed devices are added.
- Device groups are added.
- Oracle Communications Session Delivery products are loaded.
- An element is added, deleted, or modified.
- A device is rebooted.
- An HA device roles are switched.
- Configurations are saved or activated.

Security Manager

1. Expand the **Security Manager** slider and choose **Audit log > View**.
2. In the **Audit log** pane, select an entry row in the table and click **Details** or double-click the row.
3. In the **Audit log details** dialog box, the following audit trail entry is described:

Name	Description
Sequence number field	The audit log reference number.
Username field	The name of the user who performed the operation.
Time field	The time stamp for when the operation was performed by the user.
Category field	The category of operation performed by the user. For example, Authentication.
Operation field	The specific operation performed by the user.
Management Server field	The IP address of the management server accessed.
Client IP field	The IP address of the client that was used.
Device field	The IP address of the device that the user performed an operation upon.
Status field	The status of the operation performed by the user, whether it was successful or failed.
Description field	The description of the operation performed.

4. Click **OK**.
5. Click **Save to file** to open the audit log file or save it to a file.



Note: The downloaded CSV file is limited to 250 entries. Only the active page's entries are saved.

Search the Audit Log

1. Expand the **Security Manager** slider and select **Audit log > View**.
2. In the **Audit log** pane, choose an entry row in the table and click **Search**.
3. In the **Audit Log Search** dialog box, complete some or all of the following fields to search the audit log:

Name	Description
Username field	Choose the name of the user who performed the operation.
Category drop-down list	Choose the category of operation performed by the user. For example, Authentication.
Operation box	Choose the specific operation performed by the user.
Management Server	The IP address of the management server accessed.
Client IP	The IP address of the client that was used.
Device	The IP address of the device that the user performed an operation upon.
Status	The status of the operation performed by the user, whether it was successful or failed.
Start Time	Choose a start time from the calendar.
End Time	Choose an end time from the calendar.

4. Click **OK**.

Schedule Audit Log Files to Be Purged Automatically

1. Expand the **Security Manager** slider and select **Audit log > Purge**.
2. In the **Purge audit logs** pane, specify the number of days of audit logs that are kept in the **Interval in days** field.
3. Click **Apply**.

Purge Audit Log Files Manually

1. Expand the **Security Manager** slider and select **Audit log > Purge**.
2. In the **Manual Audit log purge** dialog box, click the calendar icon next to the **Purge audit log records prior to** field and choose the date from the calendar prior to which you want audit logs purged.
3. Click **OK**.

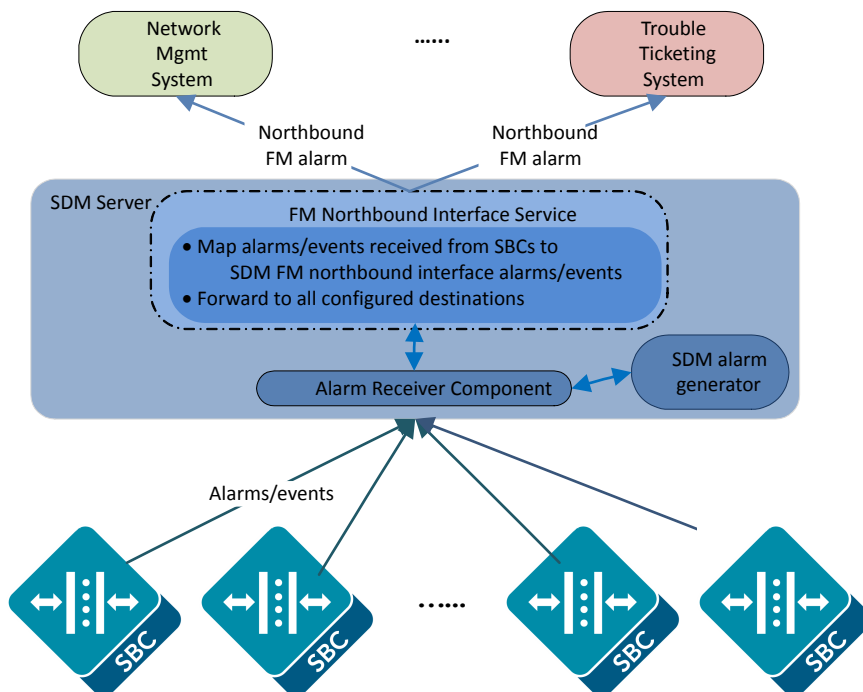
Northbound Interface

Northbound Fault Management

The Oracle Communications Session Delivery Manager Northbound Fault Management allows you to configure destination receivers to receive forwarded traps in either Oracle Communications Session Delivery Manager or ITU X.733 standard formats. You can specify selected traps on devices using the ITU X.733 format in the Add/Edit trap receiver dialog. A maximum of 10 trap receivers may be configured at once, regardless of format.

Architecture Overview

The Oracle Communications Session Delivery Manager server receives the alarms from SBCs and forwards them to selected devices.



Northbound Interface

In this diagram, the SBC sends all traps to the Oracle Communications Session Delivery Manager server, which sorts them into events and alarms. Events are the aggregated list of all such messages while alarms record only the current state or latest event. Imagine the SBC first sends a trap indicating the fan is operating at 10% and later sends a trap indicating the fan is operating at 50%. In Oracle Communications Session Delivery Manager, the alarms tab will display the trap indicating the fan is operating at 50%, whereas the events tab will display both traps.

The Fault Manager (FM) in Oracle Communications Session Delivery Manager then converts these traps to ITU X.733 format and forwards them to the selected devices.

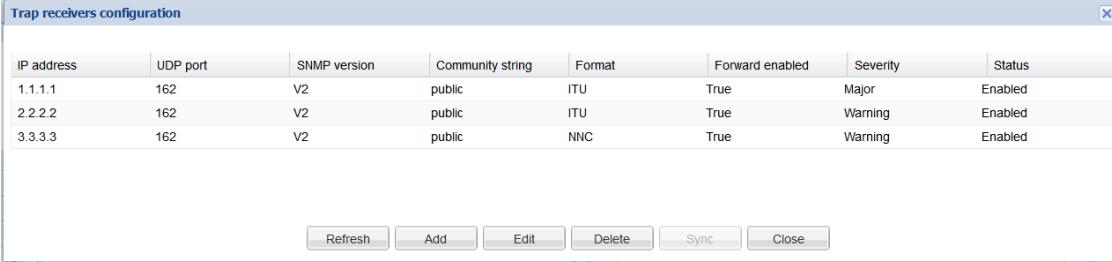
High Availability

When running Oracle Communications Session Delivery Manager within a clustered environment, northbound alarm notifications can be sent from any of the nodes in the cluster. All nodes/hosts must be specified as potential northbound alarm originators if the third-party destination requires configuring alarm originator IP addresses in an acceptance list.

All members of the cluster must share the same global identifier.

Trap Receiver Table

The trap receiver table shown below illustrates an example of configured trap receivers. The users have the ability to add/edit/delete trap receivers, as well as manually launch a process that re-synchronizes alarms for selected devices. Each operation is explained in the following sections.



IP address	UDP port	SNMP version	Community string	Format	Forward enabled	Severity	Status
1.1.1.1	162	V2	public	ITU	True	Major	Enabled
2.2.2.2	162	V2	public	ITU	True	Warning	Enabled
3.3.3.3	162	V2	public	NNC	True	Warning	Enabled

Trap Receiver Alarm Synchronization

The synchronization filter allows you to specify a window of time to synchronize alarms across devices. The Date and time from fields default to the current date and time. The Date and time to fields default to 24 hours earlier.

When enabled, the synchronization filter re-sends previous traps northbound, depending on the time window set by the user. It is up to the user to differentiate between which traps are new and which are duplicates.

Global Identifiers

You must configure a global identifier for standalone or clustered Oracle Communications Session Delivery Manager servers to satisfy the northbound managed object instance value. See the *Set the Global Identifier* section in the Typical Installation chapter of the Oracle Communications Session Delivery Manager Installation Guide for more information.



Note: The global identifier must be the same for all nodes in a clustered system.


Generic FM Northbound Notification Definition

The Fault Manager (FM) northbound interface is based on the ITU X.733 standard. In ITU X.733 terminology, a notification always originates from a managed object. A managed object is a device, service

or system that requires monitoring and management. Alarms are a specific type of notification about detected faults or abnormal conditions.

The managed object class is a category that contains one or several managed object instances of a similar type. Fan, session agent, and SipRejection are examples of managed object classes. The managed object instance, which must be able to clearly and unambiguously identify the originator of the alarm notification, is formed according to the following schema.

Managed Object Instance::=<MO_Name>.<SDMGlobalName>;<IP_address>;<MO_Detail>
MO_Name::=<ManagedObjectClassName>
SDMGlobalName::=<SDMGlobalNameString>
IP_address::= The trap originator's IP address
MO_Detail::=<ManagedObjectKeyAttrNameAndValPairs>
ManagedObjectKeyAttrNameAndValPairs::=<attrName>=<attrValue>;<attrName>=<attrValue>

 **Note:** The MO_Detail parameter of a managed object instance is empty if the alarm is singleton on a device.

The following table provides examples of the managed object instance attribute.

Description	Example of a Managed Object Instance
Alarm from the middle fan on an SBC at 172.30.80.0	Fan.nnc_srv_1;172.30.80.0;location=middle
Alarm from the session agent "sa-tge-1" on an SBC at 172.30.80.100	SessionAgent.nnc_srv_1;172.30.80.100;name=sa-tge-1
Alarm from removing a physical port on an SBC at 172.30.80.200	HotPluggablePort.nnc_srv_1;172.30.80.200;slot=01;port=01;presence=removed
Alarm in apSysMgmtGroupTrap, apSysCPUUtil, type	CPU.nnc_srv_1;172.30.80.0;apSysCPUUtil

Alarm Severity Mapping

The Oracle Communications Session Delivery Manager severity alarms are almost identical to the ITU X.733 severity alarms.

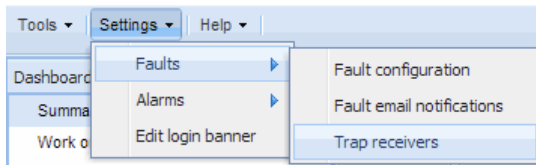
Severity	ITU X.733 Severity
Emergency/Critical	Critical
Major	Major
Minor	Minor
Warning	Warning
Clear	Clear
Unknown	Indeterminate

Accessing Northbound Fault Management Configuration

To access Northbound Fault Management configuration:

Click **Settings > Faults > Trap receivers**.

Northbound Interface



The Trap receiver table appears in the content area.

X.733 Traps to SBC Traps

This table maps the X.733 traps sent from SDM's northbound interface to the original traps sent from the SBC. The first three columns contain information found in an X.733 trap. The fourth column shows the original SBC trap which generated the alarm. Once the original trap sent by the SBC has been identified, search the documentation set for further information about that trap.

Alarms

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
H248Association	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtH248 AssociationLostTra p	H248 association
H248Association	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtH248 AssociationLostCle arTrap	H248 association
VoltageChange	EnvironmentalAl arm	EquipmentMalfunctio n	apEnvMonVoltage ChangeNotificatio n	Voltage change
CRLRRetrievalFail ure	ProcessingError Alarm	Other*	apSecurityCRLRetr ievalFailNotificatio n	CRL retrieval failure
CRLRRetrievalFail ure	ProcessingError Alarm	Other*	apSecurityCRLRetr ievalClearNotificati on	CRL retrieval failure
MediaMemory	ProcessingError Alarm	OutOfMemory	apSysMgmtMedia OutOfMemory	Media memory
MediaMemory	ProcessingError Alarm	OutOfMemory	apSysMgmtMedia OutOfMemoryClea r	Media memory
DiameterAcctServe r	Communications Alarm	CommunicationsSubs ystemFailure	apDiameterAcctSr vrDownTrap	DIAMETER Server
DiameterAcctServe r	Communications Alarm	CommunicationsSubs ystemFailure	apDiameterAcctSr vrUpTrap	DIAMETER Server
DiameterServerErr or	Communications Alarm	CommunicationsSubs ystemFailure	apDiameterSvrErr orResultTrap	Diameter server error
DiameterServerErr or	Communications Alarm	CommunicationsSubs ystemFailure	apDiameterSvrSuc cessResultTrap	Diameter server error

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
MediaPortUtilization	EquipmentAlarm	ThresholdCrossed	apSysMgmtPhyUtilThresholdTrap	Media port utilization
MediaPortUtilization	EquipmentAlarm	ThresholdCrossed	apSysMgmtPhyUtilThresholdClearTrap	Media port utilization
DatabaseRegCacheCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtDatabaseRegCacheCapTrap	System Mgmt Database Reg Cache Capacity
DatabaseRegCacheCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtDatabaseRegCacheCapClearTrap	System Mgmt Database Reg Cache Capacity
RealmIcmpFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtRealmIcmpFailureTrap	Realm Icmp Failure
RealmIcmpFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtRealmIcmpFailureClearTrap	Realm Icmp Failure
ExternalPolicyServerConnection	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtExtPolicyServerConnDownTrap	External policy server connection
ExternalPolicyServerConnection	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtExtPolicyServerConnEstTrap	External policy server connection
RadiusServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtRadiusDownTrap	RADIUS Servers
RadiusServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtRadiusDownClearTrap	RADIUS Servers
H248PortMapUsage	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtH248PortMapUsageTrap	H248 port map usage
H248PortMapUsage	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtH248PortMapUsageClearTrap	H248 port map usage
CDRPushReceiverFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtCDRPushReceiverFailureTrap	CDR Push Receiver Failure
CDRPushReceiverFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtCDRPushReceiverFailureClearTrap	CDR Push Receiver Failure
CDRPushAllReceiversFailed	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtCDRPushAllReceiversFailureTrap	CDR Push All Receivers Failed
CDRPushAllReceiversFailed	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtCDRPushAllReceiversFailureClearTrap	CDR Push All Receivers Failed

Northbound Interface

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
Rfactor	QualityOfService Alarm	ThresholdCrossed	apSysMgmtRFacto rBelowThresholdTr ap	rfactor
Rfactor	QualityOfService Alarm	ThresholdCrossed	apSysMgmtRFacto rBelowThresholdCl earTrap	rfactor
DiameterDirectorC onnection	Communications Alarm	CommunicationsSubs ystemFailure	apDdConnectionFa ilureTrap	Diameter director connection
DiameterDirectorC onnection	Communications Alarm	CommunicationsSubs ystemFailure	apDdConnectionFa ilureClearTrap	Diameter director connection
DNS- ALGServerConstra intState	operationalViolat ion	OutOfService*	apDnsAlgSvrConst raintStateChangeTr ap	DNS-ALG server constraint state
DNS- ALGServerConstra intState	operationalViolat ion	OutOfService*	apDnsAlgSvrConst raintStateChangeCl earTrap	DNS-ALG server constraint state
DNS- ALGConfiguration Constraint	operationalViolat ion	OutOfService*	apDnsAlgConstrai ntStateChangeTrap	DNS-ALG configuration constraint
DNS- ALGConfiguration Constraint	operationalViolat ion	OutOfService*	apDnsAlgConstrai ntStateChangeClea rTrap	DNS-ALG configuration constraint
NTPServer	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtNTPSe rverUnreachableTr ap	NTP server
NTPServer	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtNTPSe rverUnreachableCl earTrap	NTP server
AccountMessageQ ueue	ProcessingError Alarm	ThresholdCrossed	apAcctMsgQueueF ullTrap	Account message Queue
AccountMessageQ ueue	ProcessingError Alarm	ThresholdCrossed	apAcctMsgQueueF ullClearTrap	Account message Queue
TACACS+Servers	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtTacacs DownTrap	TACACS+ Servers
TACACS+Servers	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtTacacs DownClearTrap	TACACS+ Servers
SecondarySIPInterf aceCapacity	ProcessingError Alarm	ThresholdCrossed	apSipSecInterfaceR egThresholdExceed edTrap	Secondary SIP Interface capacity
SecondarySIPInterf aceCapacity	ProcessingError Alarm	ThresholdCrossed	apSipSecInterfaceR egThresholdClearT rap	Secondary SIP Interface capacity

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
RegistrationCache Exceeded	ProcessingError Alarm	ThresholdCrossed	apSysMgmtRegCac heThresholdTrap	Registration cache exceeded
RegistrationCache Exceeded	ProcessingError Alarm	ThresholdCrossed	apSysMgmtRegCac heThresholdClearT rap	Registration cache exceeded
MediaBandwidth	ProcessingError Alarm	ResourceAtOrNearin gCapacity	apSysMgmtMedia BandwidthTrap	Media bandwidth
MediaBandwidth	ProcessingError Alarm	ResourceAtOrNearin gCapacity	apSysMgmtMedia BandwidthClearTr ap	Media bandwidth
GTPLinkInGGSN	Communications Alarm	CommunicationsSubs ystemFailure	apSecurityGTPLin kFailureNotificatio n	Loss communication with the GGSN on a particular GTP interface
GTPLinkInGGSN	Communications Alarm	CommunicationsSubs ystemFailure	apSecurityGTPLin kClearNotification	Loss communication with the GGSN on a particular GTP interface
DiameterDirectorS CTPPathConnectio nFailure	Communications Alarm	CommunicationsSubs ystemFailure	apDdSCTPPathFail ureTrap	Diameter director SCTP Path connection failure
DiameterDirectorS CTPPathConnectio nFailure	Communications Alarm	CommunicationsSubs ystemFailure	apDdSCTPPathFail ureClearTrap	Diameter director SCTP Path connection failure
RealmMinutesExce ded	ProcessingError Alarm	ResourceAtOrNearin gCapacity	apSysMgmtRealm MinutesExceedTra p	Realm Minutes Exceeded
RealmMinutesExce ded	ProcessingError Alarm	ResourceAtOrNearin gCapacity	apSysMgmtRealm MinutesExceedCle arTrap	Realm Minutes Exceeded
AlgdCPULoad	ProcessingError Alarm	ThresholdCrossed(no Info)	apSysMgmtAlgdC PULoadTrap	CPU load
AlgdCPULoad	ProcessingError Alarm	ThresholdCrossed	apSysMgmtAlgdC PULoadClearTrap	CPU load
H323Calls	ProcessingError Alarm	ThresholdCrossed	apH323StackMaxC allThresholdTrap	H323 calls
H323Calls	ProcessingError Alarm	ThresholdCrossed	apH323StackMaxC allThresholdClearT rap	H323 calls
OCSRServers	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtOCSR DownTrap	OCSR servers

Northbound Interface

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
OCSRServers	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtOCSR DownClearTrap	OCSR servers
HDR	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtPushSe rverUnreachableTr ap	HDR
HDR	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtPushSe rverUnreachableCl earTrap	HDR
UntrustedEndpoin tCapacity	ProcessingError Alarm	ThresholdCrossed	apSLBUntrustedEn dpointCapacityThr esholdTrap	Untrusted endpoint capacity
UntrustedEndpoin tCapacity	ProcessingError Alarm	ThresholdCrossed	apSLBUntrustedEn dpointCapacityThr esholdClearTrap	Untrusted endpoint capacity
MediaPorts	ProcessingError Alarm	ThresholdCrossed	apSysMgmtMedia PortsTrap	Media ports
MediaPorts	ProcessingError Alarm	ThresholdCrossed	apSysMgmtMedia PortsClearTrap	Media ports
IPSecTunnel	ProcessingError Alarm	ThresholdCrossed	apSecurityIPsecTu nCapNotification	IPsec tunnel
IPSecTunnel	ProcessingError Alarm	ThresholdCrossed	apSecurityIPsecTu nCapClearNotificat ion	IPsec tunnel
			apSysMgmtGroup Trap	Refer to table below.
			apSysMgmtGroup ClearTrap	Refer to table below.
NTPService	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtNTPSe rviceDownTrap	NTP service
NTPService	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtNTPSe rviceDownClearTra p	NTP service
TCAThreshold	ProcessingError Alarm	ThresholdCrossed	apSysMgmtTcaTra p	TCA threshold
TCAThreshold	ProcessingError Alarm	ThresholdCrossed	apSysMgmtTcaCle arTrap	TCA threshold
EndpointCapacity	ProcessingError Alarm	ThresholdCrossed	apSLBEndpointCa pacityThresholdTra p	Endpoint capacity
EndpointCapacity	ProcessingError Alarm	ThresholdCrossed	apSLBEndpointCa pacityThresholdCle arTrap	Endpoint capacity

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
DNS-ALGServer	Communications Alarm	CommunicationsSubs ystemFailure	apDnsAlgStatusCh angeTrap	DNS-ALG server
DNS-ALGServer	Communications Alarm	CommunicationsSubs ystemFailure	apDnsAlgStatusCh angeClearTrap	DNS-ALG server
SpaceAvailability	EquipmentAlar m	ThresholdCrossed	apSysMgmtSpaceA vailThresholdTrap	Space availability
SpaceAvailability	EquipmentAlar m	ThresholdCrossed	apSysMgmtSpaceA vailThresholdClear Trap	Space availability
Gateway	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtGatew ayUnreachableTrap	Gateway
Gateway	Communications Alarm	CommunicationsSubs ystemFailure	apSysMgmtGatew ayUnreachableClea rTrap	Gateway
Hardware	EquipmentAlar m	EquipmentMalfunction	apSysMgmtHardw areErrorTrap	Hardware
SingleUnitRedund ancyConfig	EquipmentAlar m	EquipmentMalfunction	apSysMgmtSingle UnitRedundancyTr ap	Single unit redundancy config
Task	ProcessingError Alarm	SoftwareError	apSysMgmtTaskDe leteTrap	Task
License	ProcessingError Alarm	ResourceAtOrNearin gCapacity	apLicenseApproac hingCapacityNotifi cation	License
License	ProcessingError Alarm	ResourceAtOrNearin gCapacity	apLicenseNotAppr oachingCapacityN otification	License
EnumServer	Communications Alarm	CommunicationsSubs ystemFailure	apAppsENUMServ erStatusChangeTra p	Enum server
SIPInterface	ProcessingError Alarm	OutOfService	apSysMgmtInterfa ceStatusChangeTra p	SIP interface
H323Stack	ProcessingError Alarm	ConfigurationOrCust omizationError	apSysMgmtH323In itFailTrap	H323 Stack
SystemState	Other	Other	apSysMgmtSystem StateTrap	SystemState
RealmStatusChang e	ProcessingError Alarm	OoutOfService	apSysMgmtRealmS tatusChangeTrap	Realm status change
Activate-config	Other	Other	apSwCfgActivateN otification	Activate-config

Northbound Interface

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
Temperature	EnvironmentalAlarm	HeatingVentCoolingSystemProblem	apSysMgmtTempTrap	Temperature
NumberOfRejectedMessagesExceeded	ProcessingErrorAlarm	ThresholdCrossed(noInfo)	apSysMgmtRejectedMessagesThresholdExceededTrap	Number of rejected messages exceeded
CertificateSoonExpired	TimeDomainViolation	KeyExpired	apSecurityCertExpiredSoonNotification	Certificate is soon expired
CertificateExpired	TimeDomainViolation	KeyExpired	apSecurityCertExpiredNotification	Certificate is expired
IPSecCRL	SecurityServiceOrMechanismViolation	UnauthorizedAccessAttempt	apSecurityCrlInvalidNotification	IPSec CRL
MediaRealm	ProcessingErrorAlarm	UnexpectedInformation	apSysMgmtMediaUnknownRealm	Media realm
Task	ProcessingErrorAlarm	SoftwareError	apSysMgmtTaskSuspendTrap	Task
AddressDoS	OperationalViolation	DenialOfService	apSysMgmtInetAddrDOSTrap	Address DoS
MediaSupervisionTimer	TimeDomainViolation	TimingProblem	apSysMgmtMediaSupervisionTimerExpTrap	Media supervision timer
apSysLog	ProcessingErrorAlarm	Other	apSyslogMessageGenerated	apSysLog
AuthenticationFailureThreshold	SecurityServiceOrMechanismViolation	AuthenticationFailure	apSecurityAuthFailureThresholdNotification	Authentication failure threshold
EndpointIPAddressesPlacedOnAnUntrustedList	OperationalViolation	DenialOfService	apSysMgmtInetAddrTrustedToUntrustedDOSTrap	Endpoint IP address placed on an untrusted list
CallRecordingStateChange	ProcessingErrorAlarm	Other	apSysMgmtCallRecordingStateChangeTrap	Call recording state change
Fan	EquipmentAlarm	ThresholdCrossed	apSysMgmtFanTrap	Fan
Gateway	ProcessingErrorAlarm	Other	apSysMgmtGatewaySynchronizedTrap	Gateway
DoS	OperationalViolation	DenialOfService	apSysMgmtDOSTrap	DoS
ApplicationDNSServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apAppsDnsServerStatusChangeTrap	Application DNS server

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
NTPClockSkew	EquipmentAlarm	EquipmentMalfunction	apSysMgmtNTPClockSkewTrap	NTP Clock Skew
TemperatureChange	EquipmentAlarm	EquipmentMalfunction	apEnvMonTempChangeNotification	Temperature change
SataAccessError	EquipmentAlarm	EquipmentMalfunction	apSysMgmtSataAccessErrorTrap	Sata Access Error
RadiusAuthenticationRequestFailure	SecurityServiceOrMechanismViolation	AuthenticationFailure	apSecurityRadiusFailureNotification	Radius authentication request failure
SIPRejection	OperationalViolation	CallEstablishmentError	apSysMgmtSipRejectionTrap	SIP rejection
HotPlugHW	EquipmentAlarm	Other	apEnvMonPortChangeNotification	HotPlugHW
ShortSessionExceeded	OperationalViolation	ThresholdCrossed	apSysMgmtShortSessionExceedTrap	Short session exceeded
CollectorPushSuccess	Other	Other	apSysMgmtCollectorPushSuccessTrap	Collector Push Success
IPsecTunnelConnectionFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apSecurityTunnelFailureNotification	IPsec tunnel connection failure
TACACS+AuthenticationFailure	SecurityServiceOrMechanismViolation	AuthenticationFailure	apSecurityTacacsFailureNotification	TACACS+ authentication failure
EnhancedDoS	OperationalViolation	DenialOfService	apSysMgmtExpDOSTrap	Enhanced DoS
EnumConfig	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtENUMStatusChangeTrap	Enum config
EndpointIpAddressPlacedOnDenylist	OperationalViolation	DenialOfService	apSysMgmtInetAddrWithReasonDOSTrap	Endpoint IP address placed on deny-list
Redundancy	ProcessingErrorAlarm	Other	apSysMgmtRedundancyTrap	Redundancy
SecurityOCSRServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apSecurityOCSRDownNotification	Security OCSR server
SecurityOCSRServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apSecurityOCSRUpNotification	Security OCSR server
Authentication	SecurityServiceOrMechanismViolation	AuthenticationFailure	apSysMgmtAuthenticationFailedTrap	Authentication
SessionAgent	ProcessingErrorAlarm	Other	apSysMgmtSAStatusChangeTrap	Session agent

Northbound Interface

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
Power	EquipmentAlarm	EquipmentMalfunction	apSysMgmtPowerTrap	Power
Save-config	ProcessingErrorAlarm	Other	apSysMgmtCfgSaveFailTrap	Save-config
CdrFileDelete	ProcessingErrorAlarm	ResourceAtOrNearin gCapacity	apSysMgmtCdrFileDeleteTrap	Cdr File Delete
			apEnvMonStatusC hangeNotification	Refer to table below.
AdditionalLocalPo lICYLookupsLimitL xceeded	ProcessingErrorAlarm	ResourceAtOrNearin gCapacity	apSysMgmtLPLoo kupExceededTrap	Additional local policy lookups limit exceeded
I2C	EquipmentAlarm	EquipmentMalfunction	apEnvMonI2CFail Notification	I2C
IPsecTunnelFailure OnAccountOfDead PeerDetection	CommunicationsAlarm	CommunicationsSubs ystemFailure	apSecurityTunnelD PDNotification	IPsec tunnel failure on account of dead peer detection(DPD)
SurrogateRegistrati on	ProcessingErrorAlarm	Other	apSysMgmtSurrog ateRegFailed	Surrogate registration
Polling	CommunicationsAlarm	CommunicationsSubs ystemFailure	apEMSNodeUnrea chable	Polling
Polling	CommunicationsAlarm	CommunicationsSubs ystemFailure	apEMSNodeUnrea chableClear	Polling
Configuration	ProcessingErrorAlarm	Other	apEMSActivateFail ure	Configuration
Configuration	ProcessingErrorAlarm	Other	apEMSSaveFailure	Configuration
HealthMonitor	CommunicationsAlarm	CommunicationsSubs ystemFailure	apNNCServerUnre achable	HealthMonitor
HealthMonitor	CommunicationsAlarm	CommunicationsSubs ystemFailure	apNNCServerUnre achableClear	HealthMonitor
Reporting	ProcessingErrorAlarm	Other	apNNCReporting HdrDetectionFailu re	Reporting
Link	CommunicationsAlarm	CommunicationsSubs ystemFailure	linkUp	Link
Link	CommunicationsAlarm	CommunicationsSubs ystemFailure	linkDown	Link
ColdStart	EquipmentAlarm	Other	coldStart	ColdStart

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
AuthTrap	SecurityServiceO rMechanismViol ation	AuthenticationFailure	authenticationFailu re	AuthTrap
ConfigChange	ProcessingError Alarm	Other	entConfigChange	ConfigChange

apSysMgmtGroupTrap/apSysMgmtGroupClearTrap Table

ManagedObj (only MO detail portion)	Event Type	ProbableCause	Alarm_Description	(NNC Alarm) CategoryTyp e
CPU	EquipmentAlarm	ThresholdCrossed	apSysCPUUtil	CPU
MemorySD4	EquipmentAlarm	ThresholdCrossed	apEnvMonCpuCoreRamU sage	Memory SD4
CPUSD4	EquipmentAlarm	ThresholdCrossed	apEnvMonCpuCoreUsage	CPU SD4
Memory	EquipmentAlarm	ThresholdCrossed	apSysMemoryUtil	Memory
Health	EquipmentAlarm	ThresholdCrossed	apSysHealthScore	Health
Redundancy	EquipmentAlarm	Other	apSysRedundancy	Redundancy
GlobalConcurrentS ession	EquipmentAlarm	Other	apSysGlobalConSess	apSysMgmt
GlobalCPS	EquipmentAlarm	Other	apSysGlobalCPS	apSysMgmt
NATCapacity	EquipmentAlarm	ThresholdCrossed	apSysNATCapacity	NAT capacit
ARPCapacity	EquipmentAlarm	ThresholdCrossed	apSysARPCapacity	ARP capacity
LicenseCapacity	EquipmentAlarm	ThresholdCrossed	apSysLicenseCapacity	License capacity
TranscodingUtiliza tion	EquipmentAlarm	ThresholdCrossed	apSysXCodeCapacity	Transcoding utilization
AMRTranscoding Utilization	EquipmentAlarm	ThresholdCrossed	apSysXCodeAMRCapacit y	AMR transcoding utilization
AMR- WBTranscodingUti lization	EquipmentAlarm	ThresholdCrossed	apSysXCodeAMRWBCap acity	AMR-WB transcoding utilization
XCodeEVRCUtiliz ation	EquipmentAlarm	ThresholdCrossed	apSysXCodeEVRCCapacit y	XCode EVRC utilization
XCodeEVRCBUtili zation	EquipmentAlarm	ThresholdCrossed	apSysXCodeEVRCBCapac ity	XCode EVRCB utilization

Northbound Interface

ManagedObj (only MO detail portion)	Event Type	ProbableCause	Alarm_Description	(NNC Alarm) CategoryType
SystemETCCoreCPUUtilization	EquipmentAlarm	ThresholdCrossed	apSysETCCoreCPUUtil	System ETC Core CPU utilization
SystemETCMemoryUtilization	EquipmentAlarm	ThresholdCrossed	apSysETCMemoryPoolMemUtil	System ETC Memory utilization

apEnvMonStatusChangeNotification Table

ManagedObj (only MO detail portion)	Event Type	ProbableCause	Alarm_Description	(NNC Alarm) CategoryType
Phy-card	EquipmentAlarm	EquipmentMalfunction	apEnvMonPhyCardStatusIndex	Phy-card
Voltage	EquipmentAlarm	EquipmentMalfunction	apEnvMonVoltageStatusIndex	Voltage
Power	EquipmentAlarm	EquipmentMalfunction	apEnvMonPowerSupplyStatusIndex	Power
Temperature	EquipmentAlarm	EquipmentMalfunction	apEnvMonTemperatureStatusIndex	Temperature
Fan	EquipmentAlarm	EquipmentMalfunction	apEnvMonFanStatusIndex	Fan
Phy-cardSD4	EquipmentAlarm	EquipmentMalfunction	apEnvMonCardSlot	Phy-card SD4


Database Tasks

Use this chapter to perform various database tasks on your Oracle Communications Session Delivery Manager server.

Backup Command Options


Use the following command line options when issuing the backup script in the following sections to specify your database and backup destination:

- d —Specifies the directory to store the backed up file.
- all —(Default) Backs up the core database and all reporting databases. This flag is used if no other is entered.
- core —Backs up the core database only.
- report —Backs up the reporting oracle database and repository.
- ocsdmdw —Backs up the ocsdmdw oracle database.

 **Note:** You are prompted to select the backup directory upon running a backup script. The default directory can be found at: <Installation directory>/../DatabaseBackup

Backup the Database on a Shutdown Server

The following sections describe how to backup the application database on an Oracle Communications Session Delivery Manager server that is shutdown (cold backup).

 **Note:** You must have system administrator privileges on the server to do a database backup.

Shut Down the System

You can shut down the existing Oracle Communications Session Delivery Manager software version running on your system to install a new version of the software, restore a database or apply a software patch.


1. Log in as the nncentral user.
2. Change directory to the bin directory.

For example:

Database Tasks

```
cd /opt/AcmePacket/NNC75/bin
```

3. Execute the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

 **Note:** However, You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.

```
./shutdownnnc.sh
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)? Yes
```

Backup the Database on the Shutdown Server

Use this task to backup the application database on a shut down server (cold backup) to a local or remote server directory path.

1. If you are using Oracle Communications Report Manager, you must shut down the Oracle BI Publisher database instance and Oracle Report Manager database instance (OCSDMDW) before you do the cold back up of the database. See the Report Manager Administrator Operations chapter in the *Oracle Communications Report Manager Installation Guide* for more information about stopping these database instances.
2. Login to the server as the nncentral user.
3. Change to the bin directory. For example:

```
cd /opt/AcmePacket/NNC7x/bin
```

4. Enter the **backupdbcold.sh** script. For example:

```
backupdbcold.sh /<path>/ColdBackup_yyyy_mm_dd_<title>.tar.gz
```

5. Execute the **startnnc.sh** script.

```
./startnnc.sh
```

The console displays the number of services started. After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up.

6. If you are using Oracle Communications Report Manager and have shut down the Oracle BI Publisher database instance and Oracle Report Manager database instance (OCSDMDW), you must start them again. See the Report Manager Administrator Operations chapter in the *Oracle Communications Report Manager Installation Guide* for more information about starting these database instances.

Next Steps


- Check Oracle Communications Session Delivery Manager server processes.
- Begin using Oracle Communications Session Delivery Manager. Use your web browser to navigate to the server login page by entering the host name or IP address, and port number in the web browser navigation bar. For example:


```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in the *Configure User Account Passwords* section.

Backup the Database on a Running Server

Use this task to backup the application database on an Oracle Communications Session Delivery Manager server that is running (hot backup) to a local or remote server directory path.

 **Note:** You must have system administrator privileges on the server to do a database backup.

 **Note:** Contact server users to minimize or prevent their usage of the system during the backup.

1. Login to the server as the nncentral user.
2. Change to the bin directory. For example:

```
cd /opt/AcmePacket/NNC7x/bin
```


3. Enter the running server backup script and its local or remote server path:

```
backupdbhot.sh /<path>/HotBackup_YYYY_MM_DD_<title>.tar.gz
```

The backup process runs.

Restore the Database

Use this task if you need to restore the application database on your Oracle Communications Session Delivery Manager system.

 **Note:** To restore database on servers in a cluster, restore each database one at a time.

1. Login to the server as the nncentral user.
2. Change to the bin directory. For example:

```
cd /opt/AcmePacket/NNC7x/bin
```

3. If you want to perform a backup of the application database on the running Oracle Communications Session Delivery Manager server (hot backup) to a local or remote server directory path, enter the **backupdbhot.sh** script and skip to step 5. For example:

```
backupdbhot.sh /<path>/HotBackup_YYYY_MM_DD_<title>.tar.gz
```

4. If you want to perform a backup of the application database on a shut down server (cold backup) to a local or remote server directory path, use the following sub-steps:

- a) Shut down the Oracle Communications Session Delivery Manager server

 **Note:** See the *Shut Down Your System* section for more information on shutting down the Oracle Communications Session Delivery Manager server.

- b) If you are using Oracle Communications Report Manager, you must shut down the Oracle BI Publisher database instance and Oracle Report Manager database instance (OCSDMDW) before you do the cold back up of the database. See the Report Manager Administrator Operations chapter in the *Oracle Communications Report Manager Installation Guide* for more information about stopping these database instances.

- c) Enter the **backupdbcold.sh** script. For example:

```
backupdbcold.sh /<path>/ColdBackup_YYYY_MM_DD_<title>.tar.gz
```

5. Restore your system by entering the **restore.sh** script. For example:

```
restore.sh -f /opt/AcmePacket/NNC7x/bin/<title>.tar.gz
```

6. If you are using Oracle Communications Report Manager and have shut down the Oracle BI Publisher database instance and Oracle Report Manager database instance (OCSDMDW), you must start them again. See the Report Manager Administrator Operations chapter in the *Oracle Communications Report Manager Installation Guide* for more information about starting these database instances.

7. Execute the **startnnc.sh** script. For example:

```
./startnnc.sh
```

The console displays the number of services started. After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up.

Next Steps

- Check Oracle Communications Session Delivery Manager server processes.
- Begin using Oracle Communications Session Delivery Manager. Use your web browser to navigate to the server login page by entering the host name or IP address, and port number in the web browser navigation bar. For example:

```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in the *Configure User Account Passwords* section.

Backup or Restore Reporting Services for Report Manager

This task is used to backup or restore reporting services for Report Manager whether the Oracle Communications Session Delivery Manager server is running (hot backup) or shutdown (cold backup).

1. Login to the server as the nncentral user.
2. Enter the following command to restore or backup reporting services:

```
chmod -Rf g+rwX <repository_location_path>
```



Warning: If a backup of the reporting server is performed while the server is running, shutdown the WebLogic server which hosts the BI Publisher application. Ignoring this step can cause BI Publisher not to function.

3. After the backup or restore process is complete, enter the following command:

```
chown -R oracle:oracle <repository_location_path>
```

- a) If necessary, re-register BI Publisher from Oracle Communications Session Delivery Manager by deleting the existing configuration and registering to the desired running BI Publisher instance.

High Availability

Overview

High Availability (HA) enables continuous service by masking both planned and unplanned downtime and preventing single points of failure. Services remain up over 99% of the time in a given period. An HA cluster is a network of tightly linked servers that are also known as members or nodes. Fail-over clusters pool together multiple members, each of which is a candidate server for your file systems, databases or applications. Each of these systems monitors the health of other systems in the cluster.

In the event of failure in one of the cluster members, the others take over the services of the failed node. When an interruption or failure occurs in a critical application, high availability clustering will combat this by switching the operations of this application to one of the other computers or nodes within that cluster.

Session Delivery Manager HA Cluster

Oracle Communications Session Delivery Manager HA ensures that data and business processes are partitioned evenly across a cluster of Oracle Communications Session Delivery Manager servers (members or nodes) without compromising availability. It ensures reliable access to Oracle Communications Session Delivery Manager services at all times. Oracle Communications Session Delivery Manager HA cluster of redundant nodes provides continuous service even if system components fail. In the cluster, the members work together to ensure that data remains continuously available. When a fault or potential interruption does occur, the HA cluster works to quickly and seamlessly prevent a complete system failure. Because there is not one single point of failure within the cluster, operations can continue without any noticeable interruptions to the user.

While Oracle Communications Session Delivery Manager is based on a modular architecture that allows for customization, it is recommended that customers requiring a clustering solution run default configurations. See the Configure Clusters section in the Oracle Communications Session Delivery Manager Installation Guide for more information about implementing clusters in your environment.



Note: Application Orchestrator cannot run as a cluster if it is implemented with Oracle Communications Session Delivery Manager.

Terminology

Oracle Communications Session Delivery Manager HA uses the following terminology:

- **HA:** Ability of a system to provide reliable access to services to its users. Highly available services remain up over 99% of the time in a given period.

High Availability

- Co-located HA: System provides HA and high scalability using components that are geographically co-located. Further details are provided below.
- Planned downtime: Planned maintenance window that could be disruptive to system operation. Planned downtime events can include patches or re-configure components such as adding new members to a cluster or allowing members to rejoin a cluster.
- Unplanned downtime: Events that were not planned such as power outages, network, or hardware failures.
- Election: When the database master fails or becomes partitioned from the rest of the nodes in the cluster, an election is automatically held to elect a new database master. In a cluster composed of three or more nodes an election is won by the node with the simple majority of votes. Also, the node that wins an election is always the one with the most recent log records. In the case of a tie, the node with the highest priority wins. In a two node cluster, an election can be won with a single vote. The replica can be elected master if the master fails.

HA Process

Oracle Communications Session Delivery Manager clustering offers reliable access to Oracle Communications Session Delivery Manager services at all times. The cluster resilience in failure conditions provides the High Availability. The Oracle Communications Session Delivery Manager cluster accomplishes this by categorizing data into different distribution mechanisms. The following summarizes these distribution mechanisms:

- Device configuration: The device is considered as the master database for configuration data. Any member of a cluster can go to the device and retrieve the most recent configuration. This process is called on-demand loading of configuration data. Not only is the configuration on each member synchronized to the same version, this has the advantage of removing the need to replicate large datasets between members.
- Message driven data: Some data sets that can be subject to network latency such as fault management events, polling statistics and audit trails are distributed via a Message-Oriented Middleware (MOM). The MOM provides asynchronous processing that allows the Oracle Communications Session Delivery Manager systems to scale both vertically and horizontally. The resilience of the MOM is maintained via guaranteed deliveries and durable subscribers. The data is generally stored on the local host machine in a dedicated local database.
- Database replication: Sensitive data sets such as LCV, user security, and device management are transactional and need to be available across the cluster are maintained by a database replication group. The database replication group maintains one master database in the cluster at all times while all other members are replicas. Retrieval of datasets is done on the local host machines. However, transactional modifications to the data are done on the master database, which then replicates the transaction to the replicas. Replication keeps the cluster database synchronized. If the master database fails, the remaining replicas elect a new master database.
- Push-pull file transfer: Large datasets such as route sets, that are maintained in the local database or file system are transferred around the cluster via push pull mechanisms. Host members use the MOM to publish events indicating that datasets are available. The other members use SFTP to pull or push the information from or to other members in the cluster.

The Oracle Communications Session Delivery Manager HA process also guarantees execution of submitted tasks and ensures that data distribution is centralized. In order to ensure no single point of failure, a Oracle Communications Session Delivery Manager server runs a load balancer, a front-end server, and a back-end server.

- Load balancer: Entrance point to Oracle Communications Session Delivery Manager services. The load balancer provides SSL security (HTTPS), as well balancing loads among all front end servers contained in the cluster. All cluster members will run a load balancer to ensure that there is no single point of failure. Access to Oracle Communications Session Delivery Manager services is not denied as long as one Oracle Communications Session Delivery Manager server is running.

- Front end server: Responsible for maintaining the client interaction support. The front end server manages sessions and performs authentication and authorization. By default the front end server targets a local back end server.
- Back end server: Runs the services required to support any functionality provided by Oracle Communications Session Delivery Manager. For example, the back end server can provide route management, fault management, or configuration management functionality.

The back end server also hosts the embedded database service and the message service. These services are responsible for maintaining the distributed data flow and provides for redundant failover capabilities.

- Embedded database service: Framework (Berkley DB XML) that provides the database XML support for the cluster. It is an in-memory database that supports replication and seamless negotiation of allocating a master database from among all the XML database members in the cluster. The database service (DBS) provides the database functionality in the back end server. Two database instances exist on any host, one is a local database XML and the other as part of a replication group.
- Message service: Message Oriented Middleware (MOM) used in the back end server to support distributed message queues and topics. MOM is supported by the distributed event and data service (DEDS) that allows components to publish and subscribe to message topics and queues.

Co-location

All host members of a cluster must reside at the same geographical location, as well as the same IP network.

Co-located clusters must also follow these requirements:

- No firewalls can exist between the members of the cluster.
- Firewalls can exist between client browsers and the cluster members so long as the ports specified in the installation guide are exposed.
- Firewalls can exist between Oracle Communications Session Delivery product and the cluster members so long as the ports specified in the installation guide are exposed.

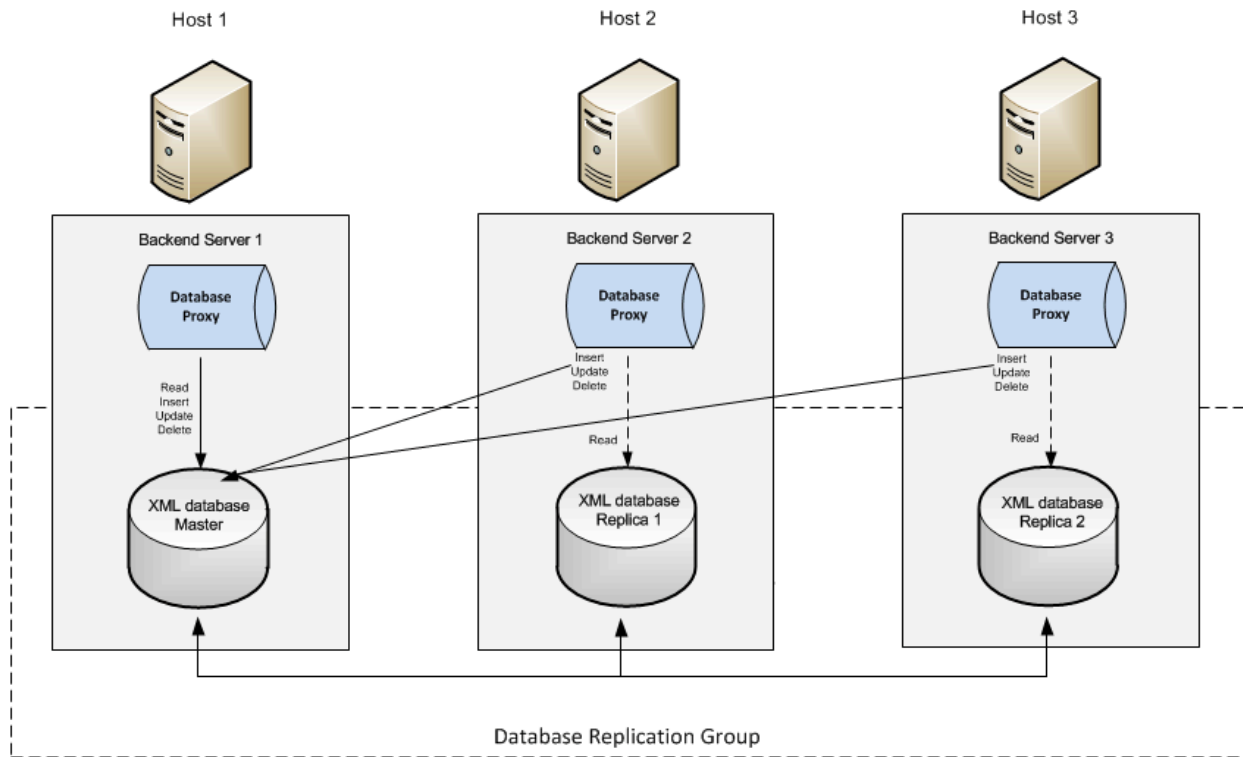
Single Master with Multiple Replica Strategy

Oracle Communications Session Delivery Manager clustering offers two distinct types of clustering configurations these are:

- Multi-member cluster
- Two-member cluster

Multi-Member Clustering

In this strategy the Oracle Communications Session Delivery Manager cluster contains three or more servers. Oracle recommends that for best HA performance and maintenance a three member cluster is configured as shown in the diagram below.



As illustrated in the diagram above, the cluster consists of three host systems. The database replication mechanism shown demonstrates the following points:

- Each host is running a backend server with an embedded-in-memory Berkeley XML database.
- In the replicated group, there is only one master database and multiple replicas.
- The master database is responsible for distribution of transactional modifications to the other replicas in the cluster.
- All back end server components interact with the database via a database proxy.
- The database proxy determines if the request for service is a transactional modification or a request for data retrieval. All data retrievals are done on the local database irrespective if it is a replica or master database. Requests for transactional modifications (inserts, updates or deletes) are forwarded from the database proxy to the master database in the cluster.
- The master database will guarantee the transactions on a quorum basis in a cluster. This means that in a cluster containing three or more members, the majority of the members need to reply that they have received the replicated datasets before the master returns success on the transaction. For example in a three member cluster the master needs to have a reply from at least one member before declaring success on the replication.
- User transactional latency is accounted for by detection of the late arrival of replicated data. Best effort replication is provided, which can mean the call might return before the dataset appears on the replicated databases. The database transactional layer offers additional support with latency in replicated data.

For example, a user on Host 3 starts a local transaction with the database proxy to insert content into the database. The database proxy in turn starts a transaction with the master database on Host 1. Each transaction that is started with the master database has a transactional id (txId) associated with it. The master database uses best effort in ensuring that the datasets are replicated to the other members of its replication group.

However, if the best effort takes longer than N seconds and the master database has received replies from quorum (the other replicas); the master database returns success. Returning success guarantees replication will occur at some point. The database Proxy on host 3 waits until the required txId appears in its local replicated database before returning success on the transaction to the user on host 3. This

guarantees that the content inserted on the Master database has reached the replicated database. Users that initiate transactions are guaranteed to see the outcome of those transactions in their local database independent of which host the original transaction was initiated.

HA for Multi-Member Cluster

In a multi member cluster, high availability is provided for as follows:

- Database replication group:

Maintains one master in the entire cluster with multiple replicas.

On master database failure, re-election among the replicated database occurs and a new master database is elected.

For three or more member cluster, transactions are deemed successful only if quorum of replies from replicas is achieved. This guarantees that the data exists on more than the master database after the transaction completes. If quorum is not met the transaction will fail.

- Messaging event and data distribution:

The MOM distributes the messages in the cluster based on a store and forward process. The MOM guarantees message delivery by storing the message in a local database first before declaring that the message was properly processed.

There is no master in the MOM cluster, all MOM brokers participating in a cluster ensure that messages are synchronized in the cluster.

Durable subscribers ensure that even if a member leaves the cluster and reenters within a 24 hour period, missed messages are re-delivered.

Tasks entered in a queue are processed even if the host where the task was originally submitted goes down.

- On-demand device configuration loading:

The device is the master database for configuration data.

No replication of large configurations is required.

Failure of a member in the host does not effect on-demand retrieval of configuration from devices serviced by other members.

Database Group Replication Data Content

Data is not compromised and is guaranteed to be replicated throughout the cluster, which ensures that failover is seamless. The data includes:

- User management data, user credentials for authentication, and user access control lists (ACL) for authorization
- User configuration modifications made per device, known as the Local Configuration View (LCV). When users make modifications to the configuration on a targeted device, only the modification changes are maintained in the LCV. This smaller dataset is replicated, reducing the latency introduced when replicating larger datasets.
- Distributed locking data. This data indicates when an Oracle Communications Session Delivery Manager lock has been placed on a targeted device for a specific operation. A distributed lock ensures that no two operations can occur concurrently on the same device.
- Oracle Communications Session Delivery product details are created when a device is added to Oracle Communications Session Delivery Manager for management. This data set provides the information required for Oracle Communications Session Delivery Manager to communicate with the targeted Oracle Communications Session Delivery product as well as provide relevant hardware, firmware, configuration and reachability status.
- Oracle Communications Session Delivery Manager configuration details. This dataset provides the user customized required configuration details that inform Oracle Communications Session Delivery Manager services on how to function.

High Availability

- Fault sequence number, which is a global unique ID required to give distributed items uniqueness.

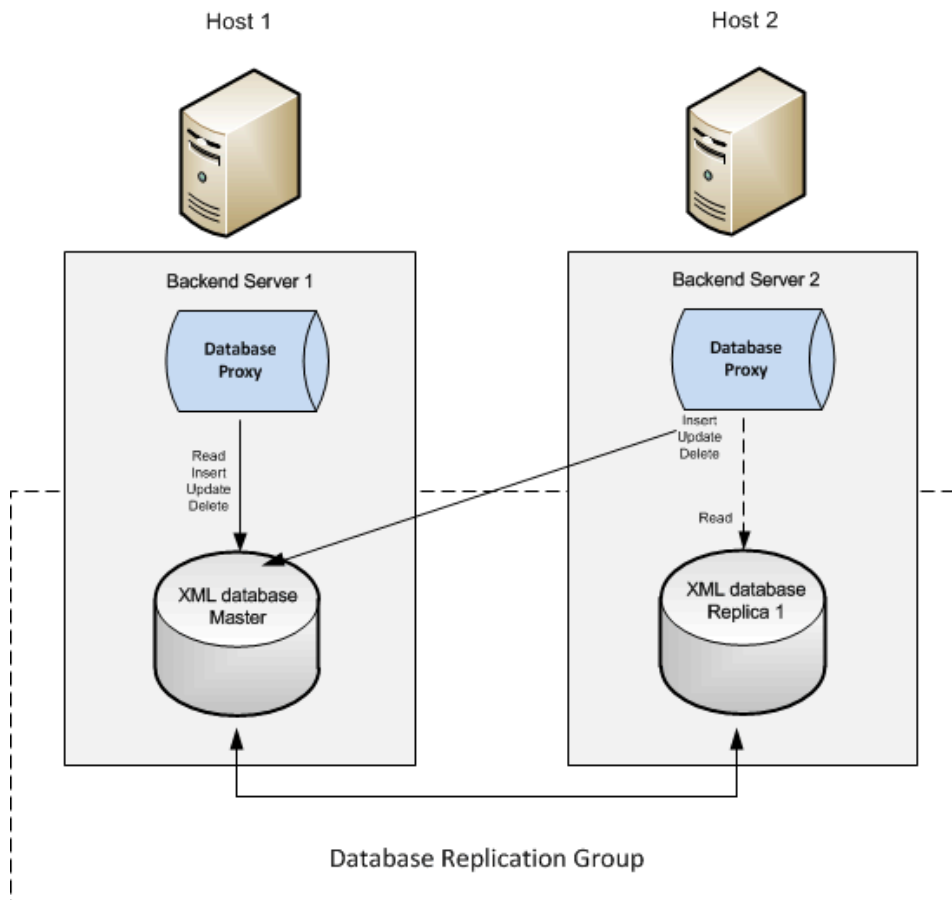
Database Group Replication HA Behavior in Multi-Member Cluster

The following table lists the activities involved in database HA behavior in a multi-member cluster.

Activity	Description
Server startup	When an Oracle Communications Session Delivery Manager server is started it joins the cluster as a replica and an election is held if there is currently no master. If the member ends up as a replica, then it is synchronized with the master during the initialization phase of the database service startup.
Master member failure	When the master fails or becomes partitioned from the rest of the members in the cluster, an election is automatically held by the remaining replicas to elect a new master.
Transactions (Quorum)	Transactions return successfully if a majority of the members in the cluster have replied that they received the replicated datasets. If quorum in replies from replicas is not achieved in a specific time period, the transaction fails.
Network partition	When a network partition exists between the members, only the members that can communicate with a majority of the members may elect a new master database. Members that can not communicate with a majority will enter READ-ONLY mode. Upon re-establishing network connectivity, re-elections take place and a master is elected while the other members revert to replicas.
Elections	In a cluster of three or more members, an election is won by the member with the simple majority of votes. The member that wins an election is always the one with the most recent log records. In the case of a tie, the member with the highest priority wins.
Rejoining a cluster after a graceful shutdown	When a server is restarted within several hours after it shuts down, the behavior is similar to the server startup activity.
Rejoining cluster after shutdown for an extended period	Perform a hot backup on the host running the master database before restarting a server that has been down for a long time. This avoids the potentially high cost synchronizing the server with the master during startup.

Two-Member Clustering

In this strategy the Oracle Communications Session Delivery Manager cluster contains only two members in the cluster as shown in the diagram below.



As illustrated in the diagram above, the cluster in this case consists of only two host machines. Considering for the moment only the database replication mechanism the following points need to be appreciated:

- Most of the items described for a three member cluster pertain here as well.
- The most important difference is that with two members the quorum policy cannot be adopted since if a network partition exists between the host machines transactions would consistently fail.
- In order to ensure transactions are serviced if a network partition exists both member will act as master databases. When the networks is re-established the members will elect which one will shut down, leaving the other to maintain services.

HA for Two Member Cluster

In a two member cluster, high availability is provided for as follows:

- Database replication group:

Maintains one master in the cluster with one replica.

On master database failure, the remaining replica becomes master.

If a network partition exists both members become masters. On re-establishing network connectivity one of the member will shutdown.

- Messaging event and data distribution:

Remains the same as described for multi member cluster

- On-demand device configuration loading:

Remains the same as described for multi member cluster

Database Group Replication HA Behavior in a Two Member Cluster

The following table lists the activities involved in database replication HA behavior in a two member cluster setup.


Server startup	When an Oracle Communications Session Delivery Manager server is started it joins the cluster as a replica and election is held if there is currently no master. If the member ends up as a replica, then it is synchronized with the master during the initialization phase of the database service startup.
Master member failure	When the master fails the remaining replica becomes the new master.
Transactions (Quorum)	Transactions return successfully if a majority of the members in the cluster have replied that they received the replicated datasets. If quorum in replies from replicas is not achieved in a specific time period, the transaction fails.
Network partition	When the master fails the remaining replica becomes the new master.
Elections	An election can be won with a single vote. This allows the replica to be elected master in the case the master fails.
Recovery after a network partition	<p>In a two node cluster it's possible for the network connection between the master and replica to be partitioned or become unresponsive due to network latency. In this situation an election is held and both nodes are elected and act as masters. While in this state, write transactions can occur at both sites. As a result, special handling is required after the partition is resolved and the system recovers from a two master configuration to a single master configuration:</p> <p>Before the partition is resolved both nodes will be in the role of master.</p> <p>After the partition is resolved an election is automatically held to elect a master.</p> <p>When the election is complete the node that wins remains the master and the other will become the replica.</p> <p>The node that loses the election and becomes the replica after previously operating as master is immediately shut down.</p> <p>The node that loses the election after a partition is resolved is shut down because the two nodes might not be in synch. All Write transactions that occurred while the nodes were partitioned cannot be automatically resolved. Only Write transactions that occurred on the node that is elected master after the partition are accepted. Because Write transactions might have also occurred on the other node, it is shutdown and must be manually synchronized with the master before it is restarted.</p>
Rejoining a cluster after graceful shutdown	An election can be won with a single vote. This allows the replica to be elected master in the case the master fails.
Rejoining cluster after shutdown for extended period	Perform a hot backup on the host running the master database before restarting a server that has been down for a long time. This avoids the potentially high cost synchronizing the server with the master during startup.

Data Synchronization Scenarios


The following sections show different data synchronization scenarios.

Add a Member to an Existing Cluster

Database backups from a standalone system cannot be restored to a cluster node. You must first configure a node as a member of the cluster before creating and restoring backed up databases. See the *Oracle Communications Session Delivery Manager Installation Guide* for details.

 **Note:** Oracle recommends adding a new member to a cluster during planned downtime.

1. Install Oracle Communications Session Delivery Manager on the server you plan to add to the cluster.
2. Run the **setup.sh** script and add all previous members in a cluster to the new member neighbor list.
3. Login to the running cluster, initiate the HM console, and record which server is running the master database.
4. Stop the replica members first, followed by the master.
5. Backup the databases on the host where the master database ran the **backupdbcold.sh** script.

 **Note:** If the member being added to the cluster contained a database at any point in time, run the **bin/reinitialize.sh** script.

6. Restore the database on the new member that is joining the cluster.
7. Run the **setup.sh** script on all other members of the cluster and add the new member to their neighbor list.
8. Start the master server first, and then the replica servers.

Member of a Cluster Fails or is Shutdown

The following describes automatic sequences that take place upon member failure or shutdown.

- Berkley DB XML: if the member leaving is running the master database, the remaining replicas carry out an election and elect a new master.
- MOM: maintain topic messages for any durable subscribers registered on the host that left. The messages would be maintained for a 24 hour period before truncation clean up occurred.
- Services that share common task processing or locks ensure that any locks acquired by the services on the member that left the cluster are cleaned up. Submitted tasks will still be processed by the remaining cluster members. Examples of these tasks include:
 - Save and Activate
 - Poller
- Clean up of any locks maintained for device synchronization. The service acquiring a lock generally provides an age-out time. If the original service cannot clean up the lock, it automatically gets aged out.
- Tasks initiated by the member that left the cluster would be re-submitted,
- Load balancers on the active hosts in the cluster bypass the front end server that has left the cluster. Clients are redirected to a valid running host.
- Health monitoring service: Health heartbeat monitor determining that a member's heartbeat has failed publishes a failed membership message to the cluster to inform all registered subscribers that a member has left the cluster.

Member Rejoining a Cluster

When a member that was previously part of a cluster rejoins that cluster, data resynchronization is required for the following databases:

- DB XML local master

High Availability

- DB XML belonging to a replication group.

Types of members rejoining a cluster include those effected by the following:

- Temporary communication outage: All cluster members are running but network issues temporarily cause members to drop connections to each other.

The tolerance window for communication outage is 8 seconds.


Because of dynamic reconnection features, a member can temporarily leave the cluster for any reason. As long as the member Oracle Communications Session Delivery Manager server has not been out of contact from the cluster for too long rejoining and re-synchronization is automatic. The Berkeley DB XML will carry out re-elections and replicate datasets to replicas. The MOM brokers send messages missed by other brokers.

- Oracle Communications Session Delivery Manager member fails or is stopped. A server fails outright and is down for some time until the administrator executes the `startnnc.sh` script. Determining how long the member has been out of contact is important:

If the member does not rejoin during the 24 hours of message storage, missed messages might not be sent to the joining broker. This server should be considered out of the cluster for extended period of time and needs to be treated as a member that needs to be re-synchronized before re-entering the cluster. If this is the case the following procedure is needed to re-join a member that has been out of the cluster for an extended period of time.

Log into the running cluster, bring up the HM console and record which server is running the master database.

Backup the databases on the host where the master database was running.

 **Note:** If the member being added to the cluster contained a database at any point in time, run the `bin/reinitialize.sh` script.

Restore the database on the member that is re-joining the cluster.


Start all Oracle Communications Session Delivery Manager servers in the cluster that includes the new member

The existing master database automatically detects a replica trying to rejoin and performs an internal initialization. Because internal initialization requires transfer of log file records that were missed to the client, it can take a lengthier period of time and could require database handles to be reopened in the replica's applications.

High Availability Scenarios

The following tasks contain summary steps for some high availability scenarios. See the *Oracle Communications Session Delivery Manager Installation Guide* and the Database tasks chapter for more detailed cluster installation information.

Retire a Cluster Member

 **Note:** Oracle recommends that you retire a member from a cluster during a planned downtime.

1. Shut down the node to be removed from the cluster.
2. Uninstall Oracle Communications Session Delivery Manager from that node.
3. Shut down all remaining nodes starting with the replicas, followed by the master.
4. Execute the `setup.sh` script.
5. Select the **Custom setup** option.
6. Select **Oracle Communications Session Delivery Manager cluster management**.
7. Enter **Yes** to continue.

8. Select **Configure** and manage members in a cluster.
9. Enter **Yes** to continue.
10. Select **Remove** to remove the first node from the cluster configuration.
11. Enter **Yes** to continue.
12. Select **Proceed** to continue removing all remote members.
13. One by one, add all members to the cluster, excluding the retired member.
14. Enter **Yes** to continue.
15. Start the master node, followed by the replicas.
After startup is complete, ensure the replications between the two nodes is in synchronicity.
16. Repeat these steps for each remaining node in the cluster.


Network Partition in Two Node Cluster

You are running a two node cluster when connectivity between the two nodes is lost. Each node elects itself as master. At this point, it is possible to lose any writes that occur to one of the databases. When the network connectivity is re-established automatically, the node that loses the election to be the master shuts down. The writes that occurred to that node are lost.

1. To re-establish the cluster, perform a hot backup on the node that is still operational.
2. Run the bin/reinitialize.sh script on the shutdown node.
3. Restore the database backup from the master onto the shutdown node.
4. Startup the shutdown node.

Network Partition in a Three Node Cluster

You are running a three or more node cluster. The network connectivity between two or more of the nodes is lost. The partition that contains a majority of the nodes elects a master from among those nodes. Any partition containing a number of servers less than the majority transitions to a READ-ONLY mode. Database updates are not permitted until the partition is resolved or the cluster has been reconfigured. A four node cluster that is partitioned into two 2 node clusters will contain two clusters running in READ-ONLY mode. When network connectivity is re-established, one node is elected master and the cluster resumes normal operation.

-  **Note:** A three-node-cluster quorum must always exist in order for a proper election to be held. Ensure that two members are always running to maintain a quorum.

Available Session Delivery Manager Server Scripts

The following Oracle Communications Session Delivery Manager server scripts are available for use by system administrators.



Note: Contact your Oracle support representative before running any scripts that are not included in the list below. Running scripts not included in the list below may affect the functionality of your deployment.

Script Location	Description
./bin/setup.sh	Launches the Oracle Communications Session Delivery Manager installation tool.
./bin/uninstall.sh	Launches the Oracle Communications Session Delivery Manager uninstall tool.
./bin/startnnc.sh	Starts the Oracle Communications Session Delivery Manager server.
./bin/shutdownnnc.sh	Shuts down the Oracle Communications Session Delivery Manager server.
./bin/showallprocesses.sh	Show all running processes on the Oracle Communications Session Delivery Manager server.
./bin/collectinfo.sh	Collects logs and system settings for the Oracle Communications Session Delivery Manager server and optionally for any database backups that occur.
./bin/reinitialize.sh	Reinitializes the database and permanently clears the data it contains.
./bin/reinitialize_ocsdmdw.sh	Reinitializes the Oracle database instance for Oracle Communications Report Manager (OCSDMDW).
./bin/backupdbcold.sh	Backs up the database on the Oracle Communications Session Delivery Manager server when it is shutdown.
./bin/backupdbhot.sh	Backs up the database on a running Oracle Communications Session Delivery Manager server.
./bin/restoredb.sh	Restores the database on the Oracle Communications Session Delivery Manager server when it is shutdown.
./bin/backup_bip.sh	Backs up the Oracle Business Intelligence (BI) Publisher database.

Available Session Delivery Manager Server Scripts

Script Location	Description
./bin/restore_bip.sh	Restores the Oracle Business Intelligence (BI) Publisher database.
./bin/ patchManagement.sh	Launches the patch management tool.