Oracle® Communications Session Delivery Manager

Administration Guide
Release 7.4
Formerly Net-Net Central

June 2015

ORACLE

Notices

Contents

About this Guide

The Oracle Communications Session Delivery Manager Installation Guide explains how to install the Session Delivery Management Suite, which provides advanced management applications and services.

NNC File and Directory Names

This guide supports Oracle Communications Session Delivery Manager Version 7.4 and subsequent 7.4 maintenance releases. File names and directories include “xx” to denote the possible presence of alphanumeric characters for maintenance releases. If you are not running a Oracle Communications Session Delivery Manager maintenance release, you can disregard the “xx”.

Below is an example of a file name for releases 7.4 and 7.4M1:

NNC74Linux64bit.tar.gz

Oracle Communications Session Delivery Manager 7.4:

- NNC74Linux64bit.tar.gz

Oracle Communications Session Delivery Manager 7.4M1:

- NNC74M1Linux64bit.tar.gz

Related Oracle Communications Session Delivery Manager Documentation

The following table lists related documents for the Oracle Communications Session Delivery Manager

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	Contains graphical and next mode installation information.
High Availability Guide	Describes Oracle Communications Session Delivery Manager High Availability (HA) and the HA cluster, which is a network of tightly-linked servers. HA provides continuous management of the SDM system.
Web Services SOAP XML Provisioning API Guide	Provides a full description of the individual interface definitions that make up the Application Programming Interface (API).
Core Functionality Guide	Contains an overview of the Oracle Communications Session Delivery Manager graphical user interface (GUI), detailed information about managing devices in Net-Net Central, and Net-Net Central licenses.
Session Element Manager Guide	Contains detailed information pertaining to the Session Element Manager application and describes the dashboard summary view, audit log, fault, and performance views.

Document Name	Document Description
Session Route Manager Guide	Contains detailed information about centrally automating the management and distribution of routing data.
Quick Start Guide	Contains a brief description of the GUI, along with information on how to add a device and perform basic configuration tasks.
Administration Guide	Contains information about security administration, which lets you create new users and new user groups, and set group-based authorization.
Report Manager Installation Guide	Contains instructions for installing Report Manager's dependencies and registering BI Publisher.
Report Manager User Guide	Contains information about configuring collection groups and creating reports.

Revision History

Date	Description
April 2014	• Initial release
July 2014	• Adds External AAA to Security Manager Chapter
June 2015	• Revisions to Security Manager Chapter • Updates to the Backup and Restore Database Chapter

1

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:

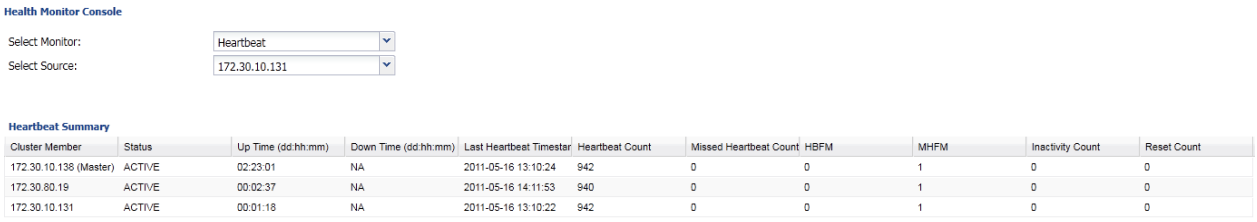
- heartbeat status information and statistics related to members of a Oracle Communications Session Delivery Manager server cluster
- server inactive and active count
- disk usage and directory statistics

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.



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.

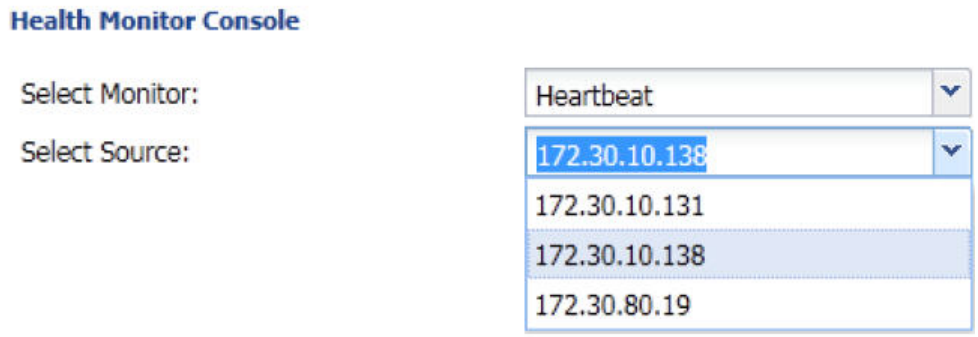
Heartbeat Monitor

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.

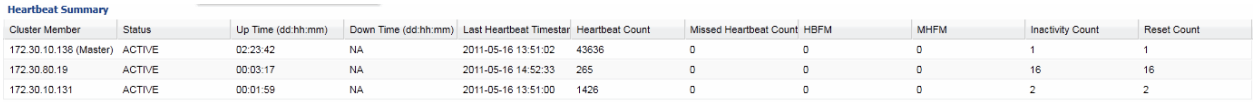
To view heartbeat statistics:

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.



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
172.30.10.136 (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
Last Heartbeat Timestamp	Date and time of the last known heartbeat for each host member as recorded by the Select member statistics being viewed.

Statistic	Description
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

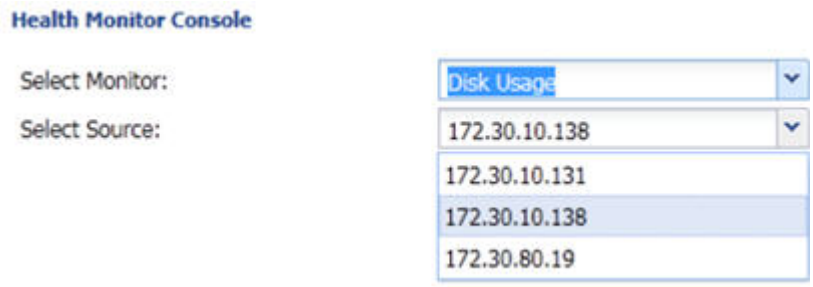
The Disk Usage Monitor maintains the statistics on disk storage usage, and checks if disk usage exceeds two threshold levels, 50% and 90% disk full. The Disk Usage monitor inspects the disk usage for the selected system and gathers statistics for total disk storage, used disk capacity, and free disk 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

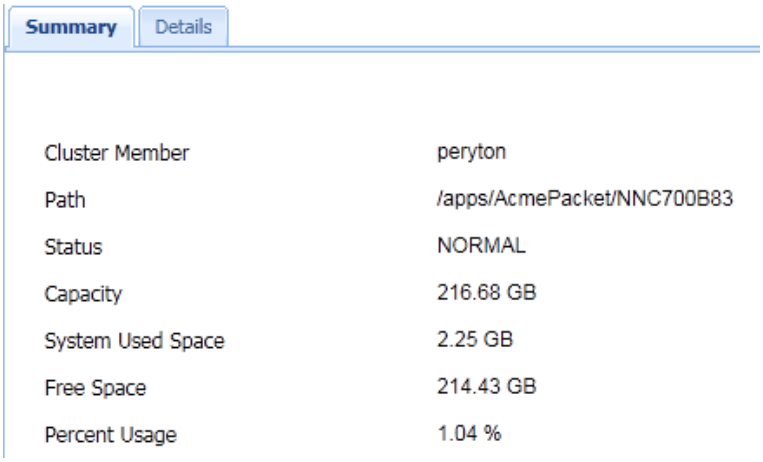
To view summary statistics:

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

2. 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.



The Disk Usage Summary view appears.



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.

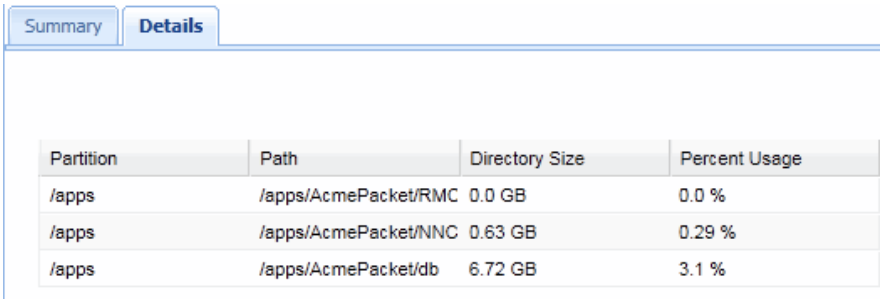
Statistic	Description
Cluster member	Name of the Oracle Communications Session Delivery Manager server
Path	Path to where Oracle Communications Session Delivery Manager is installed.
Status	Status of partition space use: Normal: below the minimum threshold value (default is 50%) Warning: at or above 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.



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

2

Security Manager

About Security Manager

A user with administrator privileges expands the **Security Manager** slider in Oracle Communications Session Delivery Manager 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.

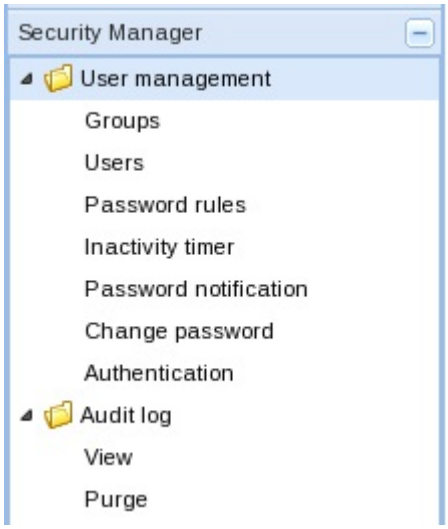


Figure 1: Security Manager Slider Parameters

Create a User Group

A user group is a logical collection of users grouped together to access common information or perform similar tasks. You assign specific permissions to a group and then assign users to it. Those users in turn, inherit the group-based permissions.

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.
   The following privilege-level categories appear for all operations in each user group in the **User Groups** table:
   - **Full**—Full authorization
   - **Partial**—Limited authorization
   - **None**—No authorization
2. In the **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	The user group name. Use the following guidelines for naming this group: • 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	Choose from the following default user groups to copy their privileges: • **None**—Manually configure permissions for this user group. • **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.

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**.

Changing Privileges for a User Group Category

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 Licensed Product Configurations

Use this task to apply user-group privileges for configurations that apply to licensed *Oracle Communications Session Border Controller* and *Oracle Communications Session Route Manager* products, and the operations Oracle Communications Session Delivery Manager uses to help apply these configurations.

Note: If you do not have licenses for the *Oracle Communications Session Element Manager* or *Oracle Communications Session Route Manager* applications, the operations on this tab do not apply.

1. On the Oracle Communications Session Delivery Manager navigation bar, choose **Security Manager** > **User management** > **Groups**.
2. In the **Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
   In the expanded group pane, the following operation category tabs appear:
3. Click the **Configuration** 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 **Configuration** tab table described below:
   - **Full**—View and modify the configuration.
   - **View**—View but not be able to modify configuration.
   - **None**—Operation does not appear in the Oracle Communications Session Delivery Manager 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 *Oracle Communications Session Element Manager* or *Oracle Communications Session Route Manager* GUIs.
Configure services item	Configure the signaling services for a *Oracle Communications Session Border Controller*. Includes SIP, DNS ALG, H.323, MGC{P, H248

Name	Description
Configure interfaces item	Configure a physical and network interfaces for a *Oracle Communications Session Border Controller*.
Configure NM controls item	Configure network management controls for multimedia traffic.
Configure security item	Configure the following *Oracle Communications Session Border Controller* security features: • 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 *Oracle Communications Session Border Controller* if licensed.
Configure system item	Configure *Oracle Communications Session Border Controller* system.
Route Management Central configuration folder	Enables *Oracle Communications Session Route Manager* 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 *Oracle Communications Session Border Controller* devices.
Create work order item	Allow user to create *Oracle Communications Session Border Controller* device upgrade operations.
Execute work order item	Allow user to execute *Oracle Communications Session Border Controller* device upgrade operations.
Load device item	Allow user to load and manage*Oracle Communications Session Border Controller* 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.
Apply to SBC folder	Save, activate, and activate saved *Oracle Communications Session Border Controller* configuration edits.
Save configuration item	Save the *Oracle Communications Session Border Controller* configuration edits made using Oracle Communications Session Delivery Manager.
Save and activate configuration item	Save and activate *Oracle Communications Session Border Controller* configuration edits made using Oracle Communications Session Delivery Manager.

Name	Description
Activate configuration item	Activate saved *Oracle Communications Session Border Controller* configuration edits made using Oracle Communications Session Delivery Manager.
Configuration archive folder	Allow user to manage the configuration archive for *Oracle Communications Session Border Controller* devices.
Back up configurations item	Allow user to back up configurations in the archive for *Oracle Communications Session Border Controller* devices.
Restore configurations item	Allow user to restore configurations in the archive for *Oracle Communications Session Border Controller* devices.
Delete archived configurations	Allow user to delete configurations in the archive for *Oracle Communications Session Border Controller* devices.

6. 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 the Administrative Operations

1. Expand the **Security Manager** slider and choose **User management** > **Groups**.
2. In the **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.

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.

Name	Description
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 *Oracle Communications Report Manager* to *Oracle Communications Report Manager*.
Change password item	Change another user's password used to login to *Oracle Communications Report Manager*.
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 *Oracle Communications Report Manager*.
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.
Add device item	Add a new device.
Remove device item	Remove an existing device.
Move device item	Move a device.
Edit login banner item	Allow users of a group to change the informational banner seen when a user logs into Oracle Communications Session Delivery Manager.
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.

Name	Description
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.
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 **Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
   In the expanded group pane, the following operation category tabs appear:
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 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 **Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
   In the expanded group pane, the following operation category tabs appear:
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: • **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.

   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**.

Apply User Group Privileges for Applications

1. Expand the **Security Manager** slider and choose **User Management** > **Groups**.
2. In the **Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
   In the expanded group pane, the following operation category tabs appear:
3. Click the **Applications** 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 **Applications** tab table described below:

   • **Full**—(Default) Allowed to perform applications operations.
   • **None**—Not allowed to perform applications operations.
   • **View**—Allowed to view applications operations.

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 *Oracle Communications Report Manager*.
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.

Name	Description
Register BI Publisher item	Set privilege levels for the *Oracle Communications Report Manager* to register with the *Oracle Communications Session Delivery Manager* before creating and running reports.

6. Click **Apply**.

Apply User Group Privileges for the Session Delivery Manager Console

1. On the Oracle Communications Session Delivery Manager navigation bar, choose **Security Manager** > **User Management** > **Groups**.
2. In the **Groups** pane, choose the group you want to modify from the **User Groups** table and click **Edit**.
   In the expanded group pane, the following operation category tabs appear:
3. Click the **Consoles** 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 **Consoles** tab table described below:
   - **Full**—(Default) Allowed to perform console operations.
   - **None**—Not allowed to perform console operations.

Name	Description
Console folder	Set privilege levels to access all console operations.
OC SDM folder	Set privilege levels to access all *Oracle Communications Session Delivery Manager* console navigation bar sliders.

6. Click **Apply**.

Create a User

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.

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: • **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

Name	Description
	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: • 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.
User information **Password** field	The password is entered for this user using the following guidelines: • 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:

Name	Description
	• **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.

Adding an Administrative User

When a device is added in the Oracle Communications Session Delivery Manager GUI, you are asked to input a user name for the device. It is possible that the user name you supply does not have administrative privileges, and therefore, certain operations are restricted. In this event, a warning message is sent:

```
Warning: the user XXX is not known by Oracle Communications Session Delivery
Manager to be an administrator on the device. Would you like to proceed? (Yes/
No):
```

By default, each device has one **admin** (administrative) user to begin. If you want to add more user names to this admin list, you must modify the sbcAdmins.conf file. The file is located in the following Oracle Communications Session Delivery Manager installation directory:

```
<NNC folder>/conf/device/sbcAdmins.conf
```

Once you modify this file by adding an administrative user, you must restart Oracle Communications Session Delivery Manager in order for the changes to be applied.

To add users to the administrative user list:

1. In Superuser mode, navigate to the file <NNC folder>/conf/device/sbcAdmins.conf.
2. Edit the sbcAdmins.conf file using any text editor.
3. Type the name to append to the admins list.
4. Save the file.

   For example:

```
# This file contains a listing of all SBC usernames NNC will consider as
admins.
# By default, this file contains just the admin username.
# To add a new username, simply append a new line containing just the
username.
admin
Robert
```

Reset a User Password

You must have permission to reset passwords.

1. Expand the **Security Manager** slider and choose **User management** > **Users**.
2. In the **Users** pane, click a user from the table and click **Reset Password**.
3. In the **Reset password** confirmation dialog box, click **Yes**.
4. In the success dialog box, click **OK**.

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	Change the assigned user group: • **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	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.
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 **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.

Cause	Action
Password deactivated	Reactivate the user account by: • 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.

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 choose **User management** > **Password rules**.
2. In the password rules pane, complete the following fields:

Name	Description
Maximum login fail attempts **For administrator users** and **For non-administrator users** fields	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 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:

Name	Description
	• **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**.

Modify the User Inactivity Timer

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 choose **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 disables the inactivity timer.
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**.

Configure When to Notify a User to Change Their Password

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

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

Note: The password notification value is applicable to all users, and this parameter cannot be set on a per-user basis.

1. Expand the **Security Manager** slider and choose **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**.

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 choose **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**.

Configure External User Authentication

External user authentication is provided through an existing RADIUS server or Active Directory (AD) server. A RADIUS server provides centralized Authentication, Authorization, and Auditing/Accounting (AAA) security protocol management for users who connect and use a network service. An AD server 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.

User groups that are created and managed externally must be mapped to internal (local) user groups. 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 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 choose **User Management** > **Authentication**.
2. In the **External authentication** pane, choose 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: • **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	**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.

Name	Description
	Choose from the following options if you want to authenticate the user with another protocol: • **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 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. • **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	This field is pre-populated with the attribute **Filter-Id** by default.  **Note:** Change the default value if the RADIUS server's group attribute does not match. 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.

4. Click **Apply**.

Configuring an Active Directory Domain Controller

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

- The Active Directory must be configured for LDAP over SSL if the Active Directory 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 choose **User Management** > **Authentication**.

2. In the **External authentication** pane, choose 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:

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 field	Choose from the following protocols used to authenticate the user: • **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. If this parameter is chosen, the additional Kerberos parameters need to be configured (see below). **Note:** If you do not choose **Kerberos**, continue to the next parameter.
Kerberos **Please choose one of Kerberos choice**	Choose one of the following Kerberos choices (if Kerberos is chosen as the password security choice): • **Choice 1**—Specify an existing krb5.conf file. • **Choice 2**—Specify a realm.
Kerberos choice 1 **Specify existing krb5. conf file** field	The Kerberos configuration 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.
Kerberos choice 2 **Kerberos realm** field	The Kerberos realm name, which is the administrative domain that encompasses all entities sharing the same database.

4. Click **Apply**.

View an Audit Log

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.

View and Save an Audit Log

1. Expand the **Security Manager** slider and choose **Audit log** > **View**.
2. In the **Audit log** pane, choose 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.

Name	Description
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 choose **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	Chose 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 choose **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 choose **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**.

3

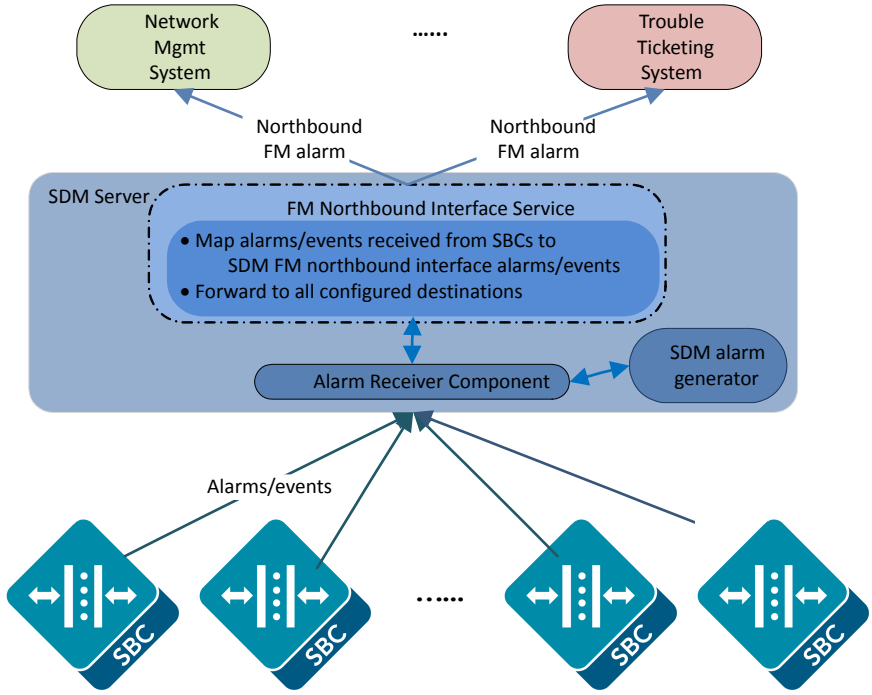
Northbound Interface

Northbound Fault Management

The Session Delivery Manager Northbound Fault Management allows you to configure destination receivers to receive forwarded traps in either SDM 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 SDM server receives the alarms from SBCs and forwards them to selected devices.



In this diagram, the SBC sends all traps to the SDM 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 SDM, 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 SDM then converts these traps to ITU X.733 format and forwards them to the selected devices.

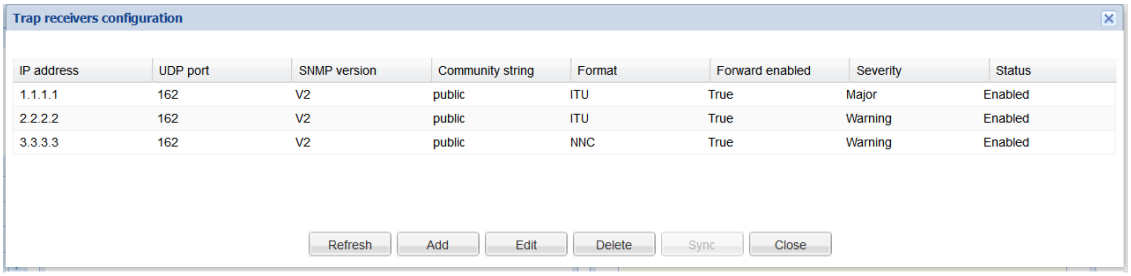
High Availability

When running SDM 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.



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 SDM servers to satisfy the northbound managed object instance value. The global identifier configuration can be found in the SDM typical and custom installation procedures.

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	HotPlugablePort.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

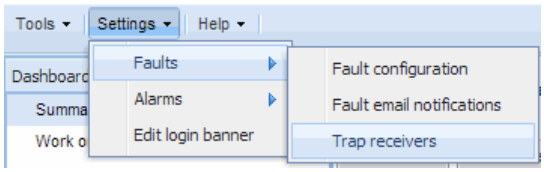
The SDM severity alarms are almost identical to the ITU X.733 severity alarms.

SDM Current 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.



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	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmntH248AssociationLostTrap	H248 association
H248Association	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmntH248AssociationLostClearTrap	H248 association
VoltageChange	EnvironmentalAlarm	EquipmentMalfunction	apEnvMonVoltageChangeNotification	Voltage change
CRLRRetrievalFailure	ProcessingErrorAlarm	Other*	apSecurityCRLRetrievalFailNotification	CRL retrieval failure
CRLRRetrievalFailure	ProcessingErrorAlarm	Other*	apSecurityCRLRetrievalClearNotification	CRL retrieval failure
MediaMemory	ProcessingErrorAlarm	OutOfMemory	apSysMgmtMediaOutOfMemory	Media memory
MediaMemory	ProcessingErrorAlarm	OutOfMemory	apSysMgmtMediaOutOfMemoryClear	Media memory
DiameterAcctServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apDiameterAcctSrvrDownTrap	DIAMETER Server
DiameterAcctServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apDiameterAcctSrvrUpTrap	DIAMETER Server
DiameterServerError	CommunicationsAlarm	CommunicationsSubsystemFailure	apDiameterSrvrErrorResultTrap	Diameter server error
DiameterServerError	CommunicationsAlarm	CommunicationsSubsystemFailure	apDiameterSrvrSuccessResultTrap	Diameter server error
MediaPortUtilization	EquipmentAlarm	ThresholdCrossed	apSysMgmtPhyUtilThresholdTrap	Media port utilization
MediaPortUtilization	EquipmentAlarm	ThresholdCrossed	apSysMgmtPhyUtilThresholdClearTrap	Media port utilization
DatabaseRegCache Capacity	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtDatabaseRegCacheCapTrap	System Mgmt Database Reg Cache Capacity
DatabaseRegCache Capacity	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtDatabaseRegCacheCapClearTrap	System Mgmt Database Reg Cache Capacity
RealmIcmpFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtRealmIcmpFailureTrap	Realm Icmp Failure

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
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
Rfactor	QualityOfServiceAlarm	ThresholdCrossed	apSysMgmtRFactorBelowThresholdTrap	rfactor
Rfactor	QualityOfServiceAlarm	ThresholdCrossed	apSysMgmtRFactorBelowThresholdClearTrap	rfactor
DiameterDirectorConnection	CommunicationsAlarm	CommunicationsSubsystemFailure	apDdConnectionFailureTrap	Diameter director connection
DiameterDirectorConnection	CommunicationsAlarm	CommunicationsSubsystemFailure	apDdConnectionFailureClearTrap	Diameter director connection
DNS-ALGServerConstraintState	operationalViolation	OutOfService*	apDnsAlgSvrConstraintStateChangeTrap	DNS-ALG server constraint state
DNS-ALGServerConstraintState	operationalViolation	OutOfService*	apDnsAlgSvrConstraintStateChangeClearTrap	DNS-ALG server constraint state

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
DNS-ALGConfigurationConstraint	operationalViolation	OutOfService*	apDnsAlgConstraintStateChangeTrap	DNS-ALG configuration constraint
DNS-ALGConfigurationConstraint	operationalViolation	OutOfService*	apDnsAlgConstraintStateChangeClearTrap	DNS-ALG configuration constraint
NTPServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtNTPServerUnreachableTrap	NTP server
NTPServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtNTPServerUnreachableClearTrap	NTP server
AccountMessageQueue	ProcessingErrorAlarm	ThresholdCrossed	apAcctMsgQueueFullTrap	Account message Queue
AccountMessageQueue	ProcessingErrorAlarm	ThresholdCrossed	apAcctMsgQueueFullClearTrap	Account message Queue
TACACS+Servers	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtTacacsDownTrap	TACACS+ Servers
TACACS+Servers	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtTacacsDownClearTrap	TACACS+ Servers
SecondarySIPInterfaceCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSipSecInterfaceRegThresholdExceededTrap	Secondary SIP Interface capacity
SecondarySIPInterfaceCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSipSecInterfaceRegThresholdClearTrap	Secondary SIP Interface capacity
RegistrationCacheExceeded	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtRegCacheThresholdTrap	Registration cache exceeded
RegistrationCacheExceeded	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtRegCacheThresholdClearTrap	Registration cache exceeded
MediaBandwidth	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtMediaBandwidthTrap	Media bandwidth
MediaBandwidth	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtMediaBandwidthClearTrap	Media bandwidth
GTPLinkInGGSN	CommunicationsAlarm	CommunicationsSubsystemFailure	apSecurityGTPLinkFailureNotification	Loss communication with the GGSN on a particular GTP interface
GTPLinkInGGSN	CommunicationsAlarm	CommunicationsSubsystemFailure	apSecurityGTPLinkClearNotification	Loss communication with the GGSN on a particular GTP interface
DiameterDirectorSCTPPathConnectionFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apDdSCTPPathFailureTrap	Diameter director SCTP Path connection failure

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
DiameterDirectorSCTPPathConnectionFailure	CommunicationsAlarm	CommunicationsSubsystemFailure	apDdSCTPPathFailureClearTrap	Diameter director SCTP Path connection failure
RealmMinutesExceeded	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtRealmMinutesExceedTrap	Realm Minutes Exceeded
RealmMinutesExceeded	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtRealmMinutesExceedClearTrap	Realm Minutes Exceeded
AlgdCPULoad	ProcessingErrorAlarm	ThresholdCrossed(noInfo)	apSysMgmtAlgdCPULoadTrap	CPU load
AlgdCPULoad	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtAlgdCPULoadClearTrap	CPU load
H323Calls	ProcessingErrorAlarm	ThresholdCrossed	apH323StackMaxCallThresholdTrap	H323 calls
H323Calls	ProcessingErrorAlarm	ThresholdCrossed	apH323StackMaxCallThresholdClearTrap	H323 calls
OCSRServers	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtOCSRDownTrap	OCSR servers
OCSRServers	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtOCSRDownClearTrap	OCSR servers
HDR	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtPushServerUnreachableTrap	HDR
HDR	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtPushServerUnreachableClearTrap	HDR
UntrustedEndpointCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSLBUntrustedEndpointCapacityThresholdTrap	Untrusted endpoint capacity
UntrustedEndpointCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSLBUntrustedEndpointCapacityThresholdClearTrap	Untrusted endpoint capacity
MediaPorts	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtMediaPortsTrap	Media ports
MediaPorts	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtMediaPortsClearTrap	Media ports
IPSecTunnel	ProcessingErrorAlarm	ThresholdCrossed	apSecurityIPsecTunCapNotification	IPsec tunnel
IPSecTunnel	ProcessingErrorAlarm	ThresholdCrossed	apSecurityIPsecTunCapClearNotification	IPsec tunnel
			apSysMgmtGroupTrap	Refer to table below.

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
			apSysMgmtGroupClearTrap	Refer to table below.
NTPService	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtNTPServiceDownTrap	NTP service
NTPService	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtNTPServiceDownClearTrap	NTP service
TCAThreshold	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtTcaTrap	TCA threshold
TCAThreshold	ProcessingErrorAlarm	ThresholdCrossed	apSysMgmtTcaClearTrap	TCA threshold
EndpointCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSLBEndpointCapacityThresholdTrap	Endpoint capacity
EndpointCapacity	ProcessingErrorAlarm	ThresholdCrossed	apSLBEndpointCapacityThresholdClearTrap	Endpoint capacity
DNS-ALGServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apDnsAlgStatusChangeTrap	DNS-ALG server
DNS-ALGServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apDnsAlgStatusChangeClearTrap	DNS-ALG server
SpaceAvailability	EquipmentAlarm	ThresholdCrossed	apSysMgmtSpaceAvailThresholdTrap	Space availability
SpaceAvailability	EquipmentAlarm	ThresholdCrossed	apSysMgmtSpaceAvailThresholdClearTrap	Space availability
Gateway	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtGatewayUnreachableTrap	Gateway
Gateway	CommunicationsAlarm	CommunicationsSubsystemFailure	apSysMgmtGatewayUnreachableClearTrap	Gateway
Hardware	EquipmentAlarm	EquipmentMalfunction	apSysMgmtHardwareErrorTrap	Hardware
SingleUnitRedundancyConfig	EquipmentAlarm	EquipmentMalfunction	apSysMgmtSingleUnitRedundancyTrap	Single unit redundancy config
Task	ProcessingErrorAlarm	SoftwareError	apSysMgmtTaskDeleteTrap	Task
License	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apLicenseApproachingCapacityNotification	License
License	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apLicenseNotApproachingCapacityNotification	License

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
EnumServer	CommunicationsAlarm	CommunicationsSubsystemFailure	apAppsENUMServerStatusChangeTrap	Enum server
SIPInterface	ProcessingErrorAlarm	OutOfService	apSysMgmtInterfaceStatusChangeTrap	SIP interface
H323Stack	ProcessingErrorAlarm	ConfigurationOrCustomizationError	apSysMgmtH323InitFailTrap	H323 Stack
SystemState	Other	Other	apSysMgmtSystemStateTrap	SystemState
RealmStatusChange	ProcessingErrorAlarm	OoutOfService	apSysMgmtRealmStatusChangeTrap	Realm status change
Activate-config	Other	Other	apSwCfgActivateNotification	Activate-config
Temperature	EnvironmentalAlarm	HeatingVentCoolingSystemProblem	apSysMgmtTempTrap	Temperature
NumberOfRejected MessagesExceeded	ProcessingErrorAlarm	ThresholdCrossed(noInfo)	apSysMgmtRejected MesagesThresholdExeededTrap	Number of rejected messages exceeded
CertificateSoonExpired	TimeDomainViolation	KeyExpired	apSecurityCertExpireSoonNotification	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
EndpointIPAddressPlacedOnAnUntrustedList	OperationalViolation	DenialOfService	apSysMgmtInetAddrTrustedToUntrustedDOSTrap	Endpoint IP address placed on an untrusted list

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
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
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

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
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
Power	EquipmentAlarm	EquipmentMalfunction	apSysMgmtPowerTrap	Power
Save-config	ProcessingErrorAlarm	Other	apSysMgmtCfgSaveFailTrap	Save-config
CdrFileDelete	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtCdrFileDeleteTrap	Cdr File Delete
			apEnvMonStatusChangeNotification	Refer to table below.
AdditionalLocalPolicyLookupsLimitLxceeded	ProcessingErrorAlarm	ResourceAtOrNearingCapacity	apSysMgmtLPLookupExceededTrap	Additional local policy lookups limit exceeded
I2C	EquipmentAlarm	EquipmentMalfunction	apEnvMonI2CFailNotification	I2C
IPsecTunnelFailureOnAccountOfDeadPeerDetection	CommunicationsAlarm	CommunicationsSubsystemFailure	apSecurityTunnelDPDNotification	IPsec tunnel failure on account of dead peer detection(DPD)
SurrogateRegistration	ProcessingErrorAlarm	Other	apSysMgmtSurrogateRegFailed	Surrogate registration
Polling	CommunicationsAlarm	CommunicationsSubsystemFailure	apEMSNodeUnreachable	Polling
Polling	CommunicationsAlarm	CommunicationsSubsystemFailure	apEMSNodeUnreachableClear	Polling
Configuration	ProcessingErrorAlarm	Other	apEMSActivateFailure	Configuration
Configuration	ProcessingErrorAlarm	Other	apEMSSaveFailure	Configuration
HealthMonitor	CommunicationsAlarm	CommunicationsSubsystemFailure	apNNCServerUnreachable	HealthMonitor
HealthMonitor	CommunicationsAlarm	CommunicationsSubsystemFailure	apNNCServerUnreachableClear	HealthMonitor
Reporting	ProcessingErrorAlarm	Other	apNNCReportingHdrDetectionFailure	Reporting

ManagedObj (only MO detail portion)	Event Type	ProbableCause	SBC Trap	(SDM Alarm) CategoryType
Link	CommunicationsAlarm	CommunicationsSubsystemFailure	linkUp	Link
Link	CommunicationsAlarm	CommunicationsSubsystemFailure	linkDown	Link
ColdStart	EquipmentAlarm	Other	coldStart	ColdStart
AuthTrap	SecurityServiceOrMechanismViolation	AuthenticationFailure	authenticationFailure	AuthTrap
ConfigChange	ProcessingErrorAlarm	Other	entConfigChange	ConfigChange

apSysMgmtGroupTrap/apSysMgmtGroupClearTrap Table

ManagedObj (only MO detail portion)	Event Type	ProbableCause	Alarm_Description	(NNC Alarm) CategoryType
CPU	EquipmentAlarm	ThresholdCrossed	apSysCPUUtil	CPU
MemorySD4	EquipmentAlarm	ThresholdCrossed	apEnvMonCpuCoreRamUsage	Memory SD4
CPUSD4	EquipmentAlarm	ThresholdCrossed	apEnvMonCpuCoreUsage	CPU SD4
Memory	EquipmentAlarm	ThresholdCrossed	apSysMemoryUtil	Memory
Health	EquipmentAlarm	ThresholdCrossed	apSysHealthScore	Health
Redundancy	EquipmentAlarm	Other	apSysRedundancy	Redundancy
GlobalConcurrentSession	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
TranscodingUtilization	EquipmentAlarm	ThresholdCrossed	apSysXCodeCapacity	Transcoding utilization
AMRTranscodingUtilization	EquipmentAlarm	ThresholdCrossed	apSysXCodeAMRCapacity	AMR transcoding utilization
AMR-WBTranscodingUtilization	EquipmentAlarm	ThresholdCrossed	apSysXCodeAMRWBCapacity	AMR-WB transcoding utilization
XCodeEVRCUtilization	EquipmentAlarm	ThresholdCrossed	apSysXCodeEVRCCapacity	XCode EVRC utilization

ManagedObj (only MO detail portion)	Event Type	ProbableCause	Alarm_Description	(NNC Alarm) CategoryType
XCodeEVRCBUtilization	EquipmentAlarm	ThresholdCrossed	apSysXCodeEVRCBCapacity	XCode EVRCB utilization
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

4

Backup and Restore Database

Backup and Restore Database Servers

If you have administrator privileges, you can back up your servers either while they are shutdown or while still running. If you want to backup a server while it is running, tell any user working on that server to minimize their usage during backup.

You can enter command line flags when issuing the back up script to specify the database and destination of the back up. By default, --all is assumed if no flag is entered.

-d — Specifies the directory to store the backed up file.

--all — Backs up core database and postgres database.

--core — Backs up core database only.

--postgres — Backs up postgres database only.

--report — Backs up reporting services only.

For Example:

```
./backupdbhot.sh --postgres
```

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

Backing Up Reporting Services

This section explains important pre-backup/restore and post-backup/restore steps for Report Manager.

1. For pre-backup/restore:
   a) Whether running a hot or cold backup or restore, run the command:

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

   b) If running a hot backup or hot restore, shutdown the WebLogic server which hosts the BI Publisher application.

   Warning: Ignoring this step will compromise BIP.

2. For post-backup/restore:
   a) After the restore process has been completed successfully, run the following command:

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

b) If necessary, re-register BI Publisher from the SDM by deleting the existing configuration and registering to the desired instance of a running BIP.

Backing Up with Server Shutdown

Backing up while the server is shutdown is a cold backup. After all backups are complete, you can restart the servers.

To back up the server while shutdown:

1. Shutdown all servers you want to backup.
2. Log in as nncentral
3. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

4. Run the coldbackup script.

```
./backupdbcold.sh
```

The backup process runs.

Backing Up with Server Running

Backing up while the server is running is a hot backup.

Note: Remember to tell any user on the server to minimize their system usage during backup.

To back up the server while running:

1. Ensure the server is running.
2. Log in as nncentral.
3. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

4. Start the hot backup script.

```
./backupdbhot.sh
```

The backup process runs.

Restoring Database Backups with Server Shutdown

You need to shutdown all servers on which you are restoring database backups. If restoring database backups on servers in a cluster, you need to restore databases on each one.

1. Shutdown all servers you plan to restore backups on.
2. Log in as nncentral.
3. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

4. Start the database restore script.

```
./restoredb.sh
```

The database restoration process runs.

Restoring Database with Server Running

Restoring a backup while the server is running is a hot restore. To restore database backups on servers in a cluster, restore the databases one at a time.

1. Log in as nncentral.
2. Change directory to NNC74/bin. For example:

```
cd /opt/AcmePacket/NNC74/bin
```

3. Start the database restore script.

```
./restoredb.sh
```

The database restoration process runs.