Oracle® Communications Session Element Manager

User Guide

Release 7.5

April 2018

Oracle Communications Session Element Manager User Guide, Release 7.5

Contents

About This Guide

Revision History xiv

1 Overview

About Session Element Manager 1-1
Accessing Session Element Manager Features through Session Delivery Manager 1-2
Customize the Display 1-3
Session Delivery Product Device Support 1-4

2 Device Manager

Configure Device Groups 2-1
- Using the Default Home Device Group 2-1
- Add a Device Group 2-1
- Move a Device Group to Another Device Group 2-2
- Rename a Device Group 2-2
- Delete a Device Group 2-2

Configure Devices 2-3
- Add One or More Devices to a Group 2-3
- Edit a Device 2-4
- Move a Device to Another Group 2-4
- Remove a Device from a Group 2-5
- Lock or Unlock a Device 2-5
- Override a Locked Device 2-5
- Reboot a Device 2-6
- Synchronize System Alarms with a Device 2-6

View Device Information 2-6
- View Device States and Columns 2-6
- Manage How Devices are Displayed 2-7
- View Hardware Details for a Device 2-8
- View Software Details for a Device 2-9
- View License Details for a Device 2-10

View Serial Numbers for a Physical Device 2-11
Export Device Information to Your Local System 2-11
Configure Device Clusters 2-12
Add a Device Cluster 2-12
Add a Device to a Device Cluster 2-13
Device Cluster Management 2-14
View Devices in a Cluster 2-14
Edit a Device Cluster 2-14
Delete a Device Cluster 2-14
Device Cluster Administrative Tasks 2-14

3 Configuration Manager

Configuration Manager Views 3-1
Navigate Between Configuration Views 3-1
Default View 3-1
ACLI View 3-2
List View 3-2
Enable Hidden Columns 3-2
Device Configuration 3-3
Associate Devices with Session Element Manager 3-3
Load the Configuration of a Local Device to Configure the Device 3-4
Load a Configuration Schema for a Device 3-4
Upload a Configuration Schema for a Device 3-5
Manage Device Configurations 3-5
View Device Data 3-7
Remove Device Data 3-7
Use Offline Configurations 3-8
Use Pre-existing Offline Configuration Templates 3-8
Copy an Offline Configuration Template 3-9
Create an Offline Configuration 3-10
Load an Offline Configuration 3-10
Create Data Variables to Support Device Specific Values 3-11
Apply an Offline Configuration 3-12
Configure and Apply Reusable Configuration Modules 3-12
Create a RCM from a Schema 3-15
Add an Element to an Existing RCM 3-15
Modify Element Properties in an Existing RCM 3-16
Pre-Define Variable Values for an Element in an RCM 3-17
Apply an RCM to a Device 3-17
Manage a Reusable Configuration Module 3-17

Load an RCM 3-17
View Reusable Configuration Modules 3-17
Update a Device Configuration 3-18
Delete an Element from an Existing RCM 3-19
Configure RCM Input Values 3-19
Delete an RCM 3-22
Manage the Configuration Archive 3-22
Add a Backup Schedule 3-23
Restore a Configuration Backup 3-24
Rename a Configuration 3-24
Search for an Archive Configuration 3-24
Manage Purge Policies 3-25
Create a Configuration Purge Policy 3-25
Purge Configurations On-Demand 3-25
Search the Archive for a Configuration 3-26
Configure Session Delivery Devices for Session Element Manager 3-27
Verify Session Delivery Product Configurations 3-27
Check Boot Parameters 3-27
Check the System Configuration Element 3-27
Check the SNMP Community Element 3-28
Check the Trap Receiver Element 3-28
Add Physical Interfaces 3-28
Configure a Physical Interface 3-29
Add a Network Interface 3-30
Configure a Network Interface 3-30
Saving and Activating Session Delivery Configurations 3-32

4 View Summary Data for Devices

Refresh Summary View Data 4-1
Refresh Data 4-1
Configure Auto Refresh 4-1
Stop Auto Refresh 4-1
View Managed Devices Data 4-2
View Key Performance Indicator Data 4-2
View Alarm Summary Data 4-3
View License Information 4-4
View Health Score Data 4-4
View Top 20 Memory Usage 4-5
View Top 20 CPU Usage 4-5
View Top 20 Alarm Counts 4-6

View Top 20 Call Rate 4-6
View Logged In Users 4-6

5 Fault Manager

Alarm and Event Configuration Tasks 5-1
Manage How Alarms are Displayed 5-1
Manage How Events are Displayed 5-3
Navigate Multiple Fault Manager Pages 5-5
Manage the Page View for Events and Alarms 5-5
Search for Alarms or Events by Specifying a Criteria 5-5
Change the Number of Alarms or Events in a Table 5-6
Save Alarms or Event Data to a File 5-6
Delete Alarms or Events 5-7
Specify a Criteria to Delete Alarms and Events 5-7
Configure When Event and Alarm Data is Cleared 5-8
Alarm Specific Configuration Tasks 5-8
Configure the Auto Refresh Period for Alarm Data 5-9
Add a Comment to an Alarm 5-9
Enable Alarm Acknowledgement 5-9
Unacknowledging Alarms 5-9
Clear an Alarm 5-10
Override Default Severity Levels for Alarm Trap Conditions 5-10
Audible Alarms 5-10
Enable and Configure Audible Alarms 5-11
Change the Default Severity Alarm Colors 5-11
Alarm Categories 5-11
Enabling Alarm Synchronization 5-13
Fault Email Notifications 5-13
Configure Email Notifications for Fault Occurrences 5-14
Delete Fault Email Notifications 5-14
Edit Fault Email Notifications 5-14
Configuring External Trap Receivers 5-15
Oracle Communications Session Element Manager Traps 5-15
Notification Objects 5-16
Add External Trap Receivers 5-16
Synchronize an External Trap Receiver to Validate the Health of a Device 5-17
Add the Heartbeat Trap to Monitor Server Availability 5-18
Edit External Trap Receivers 5-19
Delete External Trap Receivers 5-19

6 Performance Manager

View Performance Groups for a Device 6-1
Save Performance Group Data 6-2
Refresh Performance Group Data 6-3
Refresh a Performance Group 6-3
Configure the Automatic Refresh Interval for a Performance Group 6-3
Stop the Automatic Refresh of a Performance Group 6-3
View Performance Group Data 6-4
System 6-4
View General Data for a System 6-4
View Identification Data for a System 6-5
SNMP 6-6
View SNMP Performance Group Data 6-6
IP 6-8
View General IP Data 6-8
View Address Data 6-11
View Interface Statistics 6-12
View Interface Statistics Utilization Data 6-14
View Extended Interface Statistics Data 6-15
View ICMP Data 6-17
Global TCP 6-19
View TCP Data 6-20
View Global UDP Data 6-21
UDP 6-22
Environmental 6-22
View Voltage Data 6-22
View Temperature Data 6-24
View Fans Data 6-25
View Power Supply Data 6-26
View Card Data 6-27
Realms 6-28
View Current Details Data 6-28
View Average Period/State Data 6-29
View Monthly Minutes Data 6-30
View QoS Data 6-30
SIP Session 6-31
View Current SIP Session Data 6-31
View the Average Period and State of a Session 6-32
View Call Admission Control Data 6-33
H.323 Session 6-34

View Current H.323 Data 6-34
View Average Period/State Data 6-35
NSEP 6-36
View National Security Emergency Preparedness (NSEP) Data 6-36
Trap Table Summary 6-37
View Trap Table Summary Data 6-37
Storage Utilization 6-38
View Storage Utilization Data 6-38
Intrusion Detection System (IDS) 6-38
View IDS Data 6-38
Cached Contacts 6-39
View Cached Contacts Data 6-39
Network Management Controls 6-39
View NM Control Data 6-39
ENUM Servers 6-40
View ENUM Servers Data 6-40
View Codec and Transcoding Data 6-41
View Codec Data 6-41
CPU Core Table 6-42
View CPU Core Table Data 6-42

7 Device Work Orders

Preparing for a Device Work Order 7-1
User Permissions 7-1
High Availability Requirements 7-1
Software Version Requirements 7-1
Software Image Archive Management 7-2
Software Downgrade Capability 7-2
Provisioning a Device For Global Parameter Changes 7-2
Best Current Practices 7-2
Tracking Modifications in the LCV 7-2
Setting Criteria 7-3
About Device Tasks 7-3
Work Order Provisioning Cycle 7-3
Software Upgrade 7-3
Global Parameters Changes 7-4
Work Order Administration Graphical User Interface 7-5
Work Order Table 7-6
Accessing Work Order Tables 7-6
Work Order Table Actions 7-6

Work Order Table Data 7-7
Device Tasks Table 7-9
Device Task Actions 7-9
Device Task Data 7-10
Configuration and Attributes Modification Tables 7-12
Attribute Parameters Modification Table Data 7-12
Elements addition/deletion Table Data 7-12
Work Order Settings and Devices Tabs 7-13
Settings Tab 7-13
Devices Tab 7-13
Software Upgrade Work Order Administration 7-15
Software Image Archive 7-15
Work Order Administration 7-16
Global Parameter Changes Work Order Administration 7-17
Accessing Global Configuration Table 7-17
Loading a Global Configuration 7-18
GP Config Tab Actions 7-18
GP Config Tab Data 7-19
Local Configuration View (LCV) 7-19
Work Order Administration 7-19
Work Order View 7-20
Performing a Software Upgrade 7-21
Adding Software Images to the Software Image Archive Directory 7-21
Creating a Software Upgrade Work Order 7-22
Configuring Target Software Image for Software Upgrades 7-23
Configuring Optional Software Upgrade Parameters 7-23
Configuring Pause and Unlock After Loading Software Image 7-23
Configuring Break Points 7-24
Configuring Call Shedding 7-24
Configuring a Health Score for HA Pairs Only 7-24
Configuring Force Switchover to Restore Original HA Setup 7-25
Executing Work Order 7-25
Committing Work Order 7-26
Performing Global Parameter Changes 7-26
Creating a Global Configuration 7-26
Creating Global Configurations 7-26
Modifying Global Parameters 7-27
Viewing Modifications in the LCV 7-28
Viewing Attribute Parameters Modification and Elements Addition/Deletion Tables 7-28
Creating a Global Parameter Changes Work Order 7-28
Assigning the Global Configuration to the Work Order 7-29

Setting Criteria for Element Instances in Work Orders 7-30
Configuring Element Criteria 7-30
Viewing Set Criteria Details 7-32
Executing Work Order 7-32
Committing Work Order 7-32
Work Order Administration 7-32
Scheduling Work Order Start Date and Time 7-33
Configuring the Error Policy 7-33
Configuring the Behavior 7-33
Enabling Auto Commit 7-34
Adding Targeted Devices 7-35
Executing a Work Order on Demand 7-36
Commiting a Work Order 7-37
Manually Committing a Work Order 7-37
Pausing a Work Order 7-37
Resuming a Paused Work Order 7-38
Predefined Work Flows 7-38
Software Upgrade for a Standalone Device 7-38
Software Upgrade for an HA Pair 7-38
Software Rollback for a Standalone Device 7-39
Software Rollback for an HA Pair 7-39
Global Parameter Changes for a Standalone Device or an HA Pair 7-39
Global Parameter Changes Rollback for a Standalone Device or an HA Pair 7-40
Work Order Processing States and User Actions Matrices 7-40
Matrix for Work Order States and Actions 7-40
Matrix for Device Task States and Actions 7-41
Troubleshooting and Logs 7-41
Modifications Tables 7-41
Local Configuration View 7-42
Device Tasks Table 7-42
Preview Screen 7-42
Logs 7-42
Work Order Logs 7-42
Device Tasks Logs 7-43
Audit Trail Log 7-44

List of Figures

1-1 Session Delivery Manager with Session Element Manager GUI 1-3

2-1 Device groups and their associated devices 2-7

2-2 CSV file with device information 2-12

List of Tables

1 Oracle Communications Session Delivery Manager Documentation Library xiii

2 Oracle Communications Session Element Manager Documentation Library xiv

3 Oracle Communications Report Manager Documentation Library xiv

4 Oracle Communications Session Route Manager Documentation Library xiv

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: • 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.
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	• Initial release
January 2016	• Information was added to explain how Oracle Communications Session Element Manager searches and uploads a valid model XSD configuration file for a device. See the *Load a Configuration Schema for a Device* section in the Configuration Manager chapter for more information. • Information was added to customize the number of records that are displayed per page using the **Size** drop-down list, and the **All** option. See the *Customize the Display* section in the Overview chapter for more information.
February 2016	• The title of this document changed from *Oracle Communications Session Delivery Manager Element Manager* to *Oracle Communications Session Element Manager User Guide*.

Date	Description
April 2016	• The *Synchronize an External Trap Receiver* section in the Fault Manager chapter was updated. Alarms on the Oracle Communications Session Element Manager can be resent (forwarded) out of the northbound interface to the connected destination trap receiver (device) in order to synchronize alarms. • The *Add the Heartbeat Trap to Monitor Server Availability* section was added to the Fault Manager chapter to provide configuration information for the heartbeat trap (apOCSDMServerHeartbeatReachable) that is used to periodically monitor the availability of the Oracle Communications Session Element Manager from the northbound interface. • The *Create Data Variables to Support Device Specific Values* section in the Configuration Manager chapter was updated to cover the **Derive value** checkbox and **Formula** field. A derived value can be specified in cases where the data variable (DV) that you are configuring shares the same value (dependency) as another DV.
May 2016	The following changes were made in the Viewing Performance Information chapter: • The *Access Codec Data* and *Transcoding* sections were updated to add support information and a note. • The *Codec* section was renamed to *View Codec and Transcoding Data*. • The note in the *View Codec and Tanscoding Data* section was removed and a reference to the SBC documentation was added. • The *Transcoding* section was merged into the *Access Transcoding Data* section and rewritten for clarity. • The *View Transcoding Resource and Codec Statistics* section was added. • The Device Manager section was updated with across reference to the *Oracle Communications Session Delivery Manager Administration Guide* for more information regarding device clustering. • The missing *Apply an Offline Configuration* section was added to the Configuration Manager chapter.
June 2016	• The *Configure Device Clusters* section in the *High Availability* chapter of the *Oracle Communications Session Delivery Manager Administration Guide* moved to the Device Manager chapter of this guide.

Date	Description
July 2016	• The *Viewing the Audit Log* chapter was removed because it is redundant. See the *Security Manager* chapter in the *Oracle Communications Session Delivery Manager Administration Guide* for information about managing and viewing audit logs.
August 2016	• The *Viewing Performance Information* chapter was renamed *Performance Manager*. This chapter was re-organized and re-written for clarity. • The *Summary View* chapter was renamed *View Summary Data for Devices*. This chapter was re-organized and re-written for clarity. • The *Work Order Administration* chapter was renamed *Device Work Orders*.
February 2017	• Information was added to the *Navigate Configuration Manager Views* section in the Configuration Manager chapter about using the **Retrieve all** attributes check box for viewing element attribute columns.
May 2017	• Removed the *Apply RCM to a Target Global Configuration* section from the Configuration Manager chapter.
October 2017	• The *Create a Configuration Purge Policy* section was added to the *Configuration Manager* chapter.
April 2018	• The *Apply an RCM to a Device* section was added to the *Configuration Manager* chapter.

1
Overview

Oracle Communications Session Element Manager is used to manage and optimize network infrastructure elements and their functions with comprehensive tools and applications used to provision fault, configuration, accounting, performance, and security (FCAPS) support for managed devices.

About Session Element Manager

Oracle Communications Session Element Manager product is defined as the standard management application within the Oracle Communications Session Delivery Manager family of products that provides configuration, fault, performance management, and the collection and monitoring of statistical information for session delivery infrastructure elements, which includes all session delivery infrastructure products and hardware platforms.

Oracle Communications Session Element Manager is comprised of the following features, all of which are accessed through the Oracle Communications Session Delivery Manager GUI:

- **Dashboard Manager**—Use this slider to provide a dashboard summary view with at-a-glance device status and key performance indicators for your managed devices
- **Device Manager**—Use this slider to apply basic administration of individual session delivery infrastructure devices or device groups to simplify the management of small to very large networks of session delivery infrastructure product devices.
- **Configuration Manager**—Use this slider to do the following:
  - Customize your configuration of top-level elements by selecting from the following distinct configuration view styles that display a hierarchical view of session delivery infrastructure elements and their physical and logical components (physical interface, virtual interface, realm, signaling service, session agents, and so on:
    - **Default**—Display elements logically, according to the type of configuration required.
    - **ACLI**—Display media-manager, session-router, system, or security elements as they appear in the ACLI.
    - **List**—Display an alphabetically-ordered list of elements.
  - Conduct view-to-view navigation by switching from one configuration view to another, with the content area automatically refreshing to the last attribute displayed from the previous view.
  - View your own modifications made to a device through a local configuration view, which details your configuration changes.
  - Use the following folder nodes to make configuring devices easier: , and , and managing the software for multiple networks.
    - **Global Parameter**—You can make global parameter changes that enable simultaneous configuration of multiple attributes across multiple session delivery infrastructure elements.

    - **Offline Configurations**—You can use these templates to provision one or more devices without having to target each device and its elements with specific values.
    - **Reusable Modules**—You can use these work flow templates to describe a sequence of configuration changes that can be used to deploy features.
  - Use the features in the **Configure archive** folder node to perform automated and manual configuration backups for one or more elements and restore configurations from the archive. You can also audit and troubleshoot configurations to resolve problem fast and reduce maintenance costs. Its auditing capabilities include onscreen comparison of element configurations and comma-separated value (CSV) file export to save comparison results for subsequent viewing. You can also use search and sort functions on the archive and manage its size through editing and purging functions.
- **Fault Manager**—View events, alarms, and trap summary data.
- **Performance Manager**—View SNMP, IP, environmental and other performance statistics collected from Oracle Communications Session Delivery products.

Accessing Session Element Manager Features through Session Delivery Manager

1. Open your Web browser.
2. Connect to the Oracle Communications Session Delivery Manager server using one of the following address formats in the HTTP (unsecured) or HTTPS (secured) URL field of your browser to access the Oracle Communications Session Element Manager features:

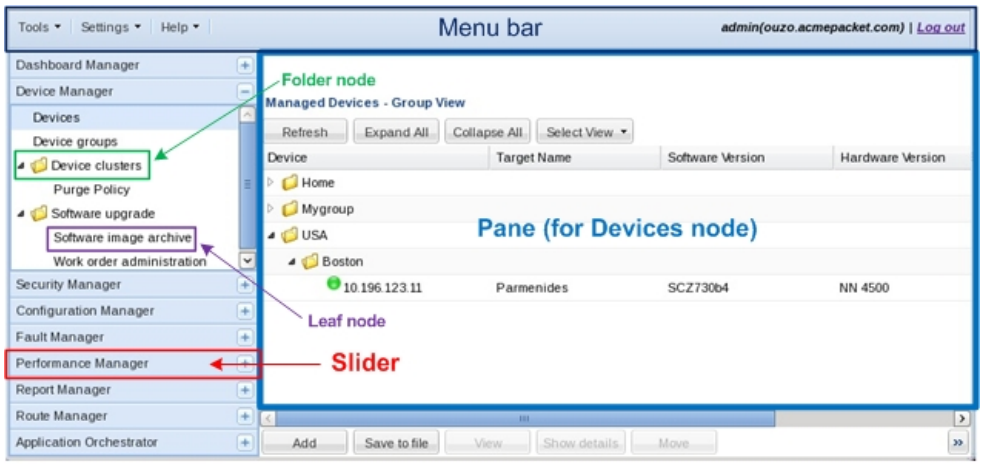
   ```
   http://<Oracle Communications Session Element Manager server IP address>:8080
   https://<Oracle Communications Session Element Manager server IP address>:
   8443
   ```

   > **Note:**
   >
   > We recommend that during the installation, you select HTTPS as the system running mode so that your system can create secure connections over the network.

3. In the **Welcome to Session Delivery Manger** login page, enter the user name and password that you configured during the installation process and click **Login**.

   The GUI for Session Delivery Manager with Oracle Communications Session Element Manager appears in the following figure:

Figure 1-1 Session Delivery Manager with Session Element Manager GUI



> **Note:**
>
> When you login to Oracle Communications Session Delivery Manager to access Oracle Communications Session Element Manager, the sliders that appear can be different depending on which applications that you have installed with Oracle Communications Session Delivery Manager. For example, Oracle Communications Application Orchestrator slider (as shown in the figure above) appears only if it was installed with Oracle Communications Session Delivery Manager.

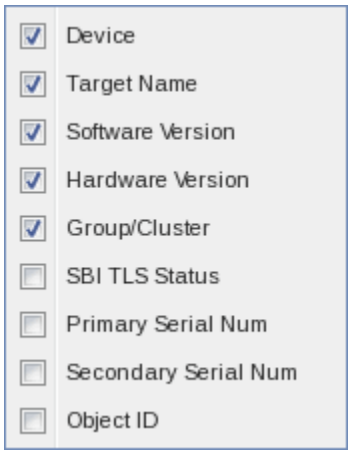
Customize the Display

Depending on the features that you use in the Oracle Communications Session Element Manager GUI, you can customize the way in which information is displayed by customizing the way table columns are displayed and table entries are ordered. You can also customize the number of records that are displayed per page.

1. Position the cursor over a column heading. An arrow appears on the right hand side of the box. For example:

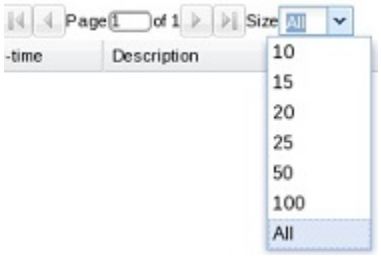
2. Click the down arrow to display the menu. For example:

3. Select **Sort Ascending** to sort the data in ascending order or **Sort Descending** to sort the data in descending order.
4. Select **Columns** to access a list of column names. For example:



5. Click a marked checkbox to hide that column or click an empty checkbox to display that column. The display view automatically updates.
6. To display a page of records that you want to view, you can use the buttons to move between pages or enter the page number you want.
7. To customize the number of records that are displayed per page, click the **Size** drop-down list.

> **Note:**
>
> If you cannot sort table columns using the **Sort Ascending** or **Descending** column options, select the **All** option from the **Size** drop-down list in order to use these column options. For example, the **All** option appears in the **Size** drop-down list when you load a device in Configuration Manager to display records for the **local-policy** configuration element. If you are having trouble sorting the column order for this configuration element, use the **All** option and try again.



8. Click elsewhere in the display to clear the menus.

Session Delivery Product Device Support

The Oracle Communications Session Element Manager application allows you to load, configure, and manage the following Oracle Communications session delivery devices:

- C-Series—Also known as the AP4000 series and AP3000 series. The AP4000 series contains the AP4250, AP4500, and AP4600. The AP3000 series contains the AP3800 (Sku 3810) and AP3820.

- D-Series—Also known as the AP9000 series, it contains the AP9200 only.
- E-Series—Also known as the AP2000 series, it contains the AP2600 only.

> **Note:**
>
> See the *Configure Oracle Communications Session Delivery Products* section of the *Configuration Manager* chapter in this guide for more information about managing session delivery devices.

2
Device Manager

The **Device Manager** slider is used to add, manage, and view Oracle Communications session delivery product devices that are deployed in your network.

You can assign individual devices to a device group, which is a logical grouping of devices managed by Oracle Communications Session Element Manager. Device groups can be set up and maintained at any level in a hierarchy that can contain any number of levels according to the needs of your organization. User permissions can be managed based on operation and device group privileges. Summary and detailed information can be displayed for individual devices and device groups.

The **Device Manager** slider contains the following nodes and folder nodes:

- **Devices**—Add, manage, and remove managed devices to Oracle Communications Session Delivery Manager.
- **Device Groups**—With the appropriate permissions, you can add, manage, rename and remove device groups.
- **Device Clusters**—Add devices to a cluster, manage devices belonging to a cluster, and remove devices from clusters that share the same hardware, software, and configuration. See the *Configure Device Clusters* section in the High Availability chapter of the *Oracle Communications Session Delivery Manager Administration Guide* for more information.
- **Software Upgrade**—Upgrade the software of devices.

Configure Device Groups

You can add or manage device groups before you add devices to them.

Using the Default Home Device Group

You can add your devices to the default **Home** device group if no other groups need to be created. Use this group with the following conditions:

- You must be assigned administrative privileges to view this device group.
- You cannot rename this device group.
- You cannot delete this device group.
- When adding a device, the **Home** device group displays in the **Add Device Group** dialog box only if you have not targeted a previous device group from the table.

Add a Device Group

Use the following naming conventions when you add a device group:

- It must start with an alphabetic character.
- It can contain a minimum of three characters and a maximum of 50 characters.

- It can contain the following characters: alphabetic, numeric, hyphens (-), and underscores (_).
- It can be a mix of upper-case and lower-case characters.
- It cannot contain symbols or spaces.
- It cannot be the same name as an existing group name within the same level in the hierarchy (sibling).

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device Groups** pane, click **Add**.
3. In the **Add device group** dialog box, enter the name for the device group in the **Device group name** field and click **OK**.

   The device group now appears in the **Device Groups** pane.

Move a Device Group to Another Device Group

When a device group is moved, all devices within that device group are moved.

> **Note:**
>
> A device group cannot be moved into one of its child groups.

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device Groups** pane, click the device group you want to move and click **Move**.
3. In the **Move device group(s) to** dialog box, click the device group in which you want to move your device group and click **OK**.

Rename a Device Group

You can rename a device group if it does not belong to another device group at the same hierarchical level.

1. Expand the **Device Manager** slider and click **Device Groups**.
2. In the **Device groups** pane, select the device group you want to rename and click **Rename**.
3. In the **Rename device group** dialog box, enter the new name in the **Rename device group to** field and click **OK**.

   The new name appears in the **Device Groups** pane.

Delete a Device Group

You can delete a device group (folder) from the **Device Groups** list with the appropriate permissions, and under the following conditions:

- Empty the device group folder and move all devices to another device group folder or delete the devices from the device group folder in order to delete the device group folder.
- You cannot delete a device group if it causes a duplicate device group in the tree hierarchy.

1. Expand the **Device Manager** slider and click **Device Groups**.

2. In the **Device Groups** pane, click the device group and click **Delete**.
3. In the **Delete device group** confirmation dialog box, click **Yes** to delete the device group.
4. In the success dialog box, click **OK**.

Configure Devices

Use Device Manager to add Oracle Communications session delivery product devices to the device groups that you created, manage devices in various ways, and view device information and how devices are displayed.

Add One or More Devices to a Group

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click **Add**.
3. In the **Add Device** dialog box, complete the following fields:

Name	Description
IP address 1 field	Enter the IP address for this device.
IP address 2 field	Enter the IP address for the second device, if this device is part of a cluster.
User Name field	The user name used to login to the device.
User Password field	The password used to login to the device.
SNMP community name field	Enter the SNMP community name for this device, which is the name of an active community where the device can send or receive SNMP performance and fault information. **Note:** The SNMP community must be configured on the device before adding the device to the Session Delivery Manager. Use the device CLI to configure the **ip-addresses** parameter found in the **configure terminal** > **system** > **snmp-community** element. For more information, See the *SNMP Community Configuration* section in the *System Configuration* chapter of the *ACLI Configuration Guide*.
SNMP port field	The default value is 161. Enter a new SNMP port number if you want.
Device Group field	Click the ellipsis button (...). In the **Set Device Group** dialog box, select the device group to which you want this device to belong. The device group now displays in the field.

Name	Description
2600 device information check box	If your device is an Oracle® Communications Application Session Controller, check the check box and parameters listed below become available.
Web protocol drop-down list	Select either HTTP (unsecure) or HTTPS (secure) for the Web protocol.
Web port field	The default value is 80. Enter a new valid Web port number if you want.
Web Services protocol drop-down list	Select either HTTP (unsecure) or HTTPS (secure) for the Web services protocol.
Web Services port field	The default value is 80. Enter a new valid Web port number if you want.

4. You can either click **OK** to add the device (if you are adding only one device) to a device group in Oracle Communications Session Element Manager or continue to the next steps if you are adding more than one device.
5. Click **Apply. Add more?** to continue to add devices.

   The **Add Device** dialog box remains open with your originally-entered values, but the last octet of the management IP address is cleared so you can rapidly add a number to the last octet for another device. For example, 172.30.80.**112**, 172.30.80.**125**, and so on. You can also change the device type by selecting a different device type from the **Device type** drop-down list.

Edit a Device

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click **Edit**.
3. In the **Edit Device** dialog box, change the appropriate parameters.
4. Click **OK** to finish editing the device.

Move a Device to Another Group

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** page, click a device group to expand the list of devices within the group.
3. Click to select the device you want to move from one device group to another and click **Move**.
4. In the **Move Device** dialog box, click to select the device group you want the device to belong and click **OK**.
5. In the **Success** dialog box, click **OK**.

Remove a Device from a Group

> **Note:**
>
> You cannot remove a device during a configuration update or if the device is locked unless you are the owner of the lock or an administrator overrides the lock. An error message appears in both situations.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** page, click a device group to expand the list of devices within the group.
3. Click to select the device you want to remove and click **Remove**.
4. In the **Remove device** dialog box, click **Yes**.

Lock or Unlock a Device

You can lock or unlock a device with the appropriate administrator permissions.

> **Note:**
>
> Other users are prevented from rebooting, updating or modifying the configuration or route sets for a device when you lock it. Only users with granted override lock permissions can override your lock or the device must be unlocked by you.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click the device you want to lock and click **Lock** if it is unlocked or **Unlock** if it is locked.
3. In the confirmation dialog box, click **Yes**.

   A padlock icon appears next to the IP address of the device. This padlock is removed if the device is unlocked.

Override a Locked Device

> **Note:**
>
> You must have the appropriate privileges assigned by your administrator to override a lock set on a device by another user.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click the device you want to override lock and click **Admin**.
3. From the **Admin** pop-up menu, select **Override lock**.

4. In the **Confirm** dialog box, click **Yes**.
5. In the **Managed Devices** pane, click **Refresh**.

   The padlock icon no longer appears next to the IP address of the device.

Reboot a Device

> **Note:**
>
> You must have the appropriate administrator permissions assigned to reboot a device.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select the device you want to reboot, and click **Admin**.
3. In the **Admin** drop-down list, click **Reboot**.
4. In the **Confirm** dialog box, click **Yes**.
5. Once you see the reboot process finish in the **Progress** dialog box, click **Close**.
6. In the **Reboot Device** dialog box, click **OK**.

   > **Note:**
   >
   > This dialog box confirms that the reboot process has completed successfully.

Synchronize System Alarms with a Device

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click the device you want to synchronize with system alarms and click **Admin**.
3. From the drop-down list, click **Synchronize alarms**.
4. In the **Synchronize alarms** dialog box, click **Yes**.
5. In the Information dialog box that displays, click **OK**.

View Device Information

Use the following sections to view Oracle session delivery product device information, manage the way device information is displayed, and show detailed device information.

View Device States and Columns

You can monitor a variety of information for Oracle session delivery product devices by viewing the state of their colored, round icons, and using the column information presented for each device.

Expand the **Device Manager** slider and click **Devices**. A device group hierarchy displays the group folders and group subfolders for the devices they contain, as shown in the example below.

Figure 2-1 Device groups and their associated devices

Device	Target Name	Software Version	Hardware Version
Home			
10.196.123.15	ACMEPACKET	SCX630m5p9	NN 3820
10.196.123.16	ACMEPACKET	SCX640	NN 3820
USA			
Boston			
10.196.123.11	Parmenides	SCZ730b4	NN 4500

The following states of a device in the **Managed Devices** table indicate if it can be reached by Oracle Communications Session Element Manager:

- Green—The device (or both devices in a cluster) is reachable by Oracle Communications Session Element Manager and information for this device can be retrieved through SNMP.
- Red—Oracle Communications Session Element Manager cannot currently contact the device (or cannot contact both devices in a cluster).
- Yellow—The standby device in the cluster is not reachable by Oracle Communications Session Element Manager.

The following columns appear in the **Managed Devices** table for each device:

Name	Description
Device	The IP address of the standalone device or each device in a cluster.
Target Name	The user-defined name for each device.
Software Version	The full release version, including patch number, of software on device.
Hardware Version	The full hardware platform identification.
Group/Cluster	Associated Device Cluster name when in Group View or associated Device Group name when in Cluster View.
SBI/TLS Status	(Hidden) Status of TLS on device ACP communications.
Primary Serial Num	(Hidden) Serial number of the standalone device or the primary device in an HA deployment.
Secondary Serial Num	(Hidden) Serial number of the secondary device in an HA deployment.
Object ID	(Hidden) Internal database object ID.

Manage How Devices are Displayed

Use the buttons at the top of the **Managed Devices** pane to affect the display of device information.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, you can use the following buttons to manage how devices are displayed:

Name	Description
Refresh	Click to refresh the data displayed on the screen for this device.
Expand All	Click to expand all device group folders.
Collapse All	Click to collapse all device group folders.
Select View	Click to select the following operations from the drop-down menu: • **Group View**—Select to display devices grouped by their associated device group. • **Cluster View**—Select to display devices grouped by their associated cluster.

View Hardware Details for a Device

You can find the following component inventory data for your device, such as chassis, CPU, memory, and so on.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click to select the device for which you want to show details and click **Show details**.
3. In the **Hardware** tab, the following columns display for a standalone devices, or for devices that belong to a cluster:

Name	Description
Index	(Hidden) The number assigned to each component of the device.
Description	The text description of the physical entity.
Vendor type	The vendor-specific hardware type of the physical entity. **Note:** This value is different from the definition of MIB-II sysObjectID.
Contained in	(Hidden) The index number in which this hardware component is contained.
Class	The enumerated value that indicates the general hardware type of this physical entity.
Name	Textual name of this physical entity. Name of the component as assigned by the local device.
Hardware Rev	The vendor-specific hardware revision string for the physical entity.
Firmware Rev	The vendor-specific firmware revision string for the physical entity.
Manufacturer	The name of the manufacturer of this physical entity.
Model Name	The vendor-specific model name identifier string associated with this physical entity.

Name	Description
Is FRU	This indicates whether this physical entity is considered a field replace unit (FRU) by the vendor.
Serial Number	The serial number of the chassis or module.

View Software Details for a Device

The following boot parameters are displayed for Oracle Communications session delivery product devices:

- The software image and where the image is booted for this device (on an external device or internal flash memory).
- The type of software entity being booted.
- Status of that software entity.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click to select the device for which you want to show details and click **Show details**.
3. In the **Device details** pane, click the **Software** tab. The following fields, boot table and backup table columns display:

Name	Description
Current configuration version field	The saved version number of the current configuration image.
Running configuration version field	The saved version number of the configuration currently running on the Oracle Communications session delivery product.
Index column	(Hidden) The number assigned to each software image on the device.
Description column	The software image name, device location, IP address or other unique identifiers. For example: • host address/image name (boot image) 10.0.1.12/sd121p3.gz • boot from flash0/image name (boot image) /tffs0/sd121p3.gz • bank0:date time (boot loader) bank0:06/13/2005 10:58:25
Type column	The software entity type. Values are: • **bootImage** • **bootLoader**
Status column	This column describes whether the software image is currently used or previously used.
Backup column	The Oracle Communications Session Delivery product device can save an existing configuration into a single backup file. Backups are created as gzipped tar files in a .tar.gz format. They are stored in the /code/bkups directory on the Oracle Communications session delivery product device.

View License Details for a Device

Many components of the Oracle Communications session delivery product device software are licensed by Oracle and some product devices require a license key. Products using the newer license entitlements feature do not have entries in this area.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click to select the device for which you want to show details and click **Show details**.
3. In the **Device details** pane, click the **License** tab. The following field and table columns display:

Name	Description
Total capacity field	The total capacity for the device, which is the maximum number of simultaneous sessions allowed by this device for all combined protocols. If the device has undergone several license upgrades, the value of each capacity row adds up to the total capacity value.
License Key column	The license number.
Capacity column	The maximum number of simultaneous sessions allowed by the device for all combined protocols.
Install Date column	The installation time and date when the software was installed on the device. **N/A** appears if a license is not enabled.
Begin Date column	The beginning time and date when the software was licensed on the device. **N/A** appears if a license is not enabled.
Expire Date column	The end time and date when the software license expired on the device. **N/A** appears if a license is not enabled.
Protocol Names column	All protocols licensed for this device. Values are: SIP, MGCP, and H.323.
Feature Namescolumn	The following features can be licensed for this device: • Interworking (IWF) • Quality of Service (QoS) • Acme Control Protocol (ACP) • Local Policy (LP) • Session Agent Group (SAG) • ACC—Enables Oracle Communications session delivery product devices to create connections, and send CDRs to one or more RADIUS servers). • High Availability (HA)

View Serial Numbers for a Physical Device

Primary and secondary serial numbers of managed physical devices can be displayed by enabling hidden columns in the **Managed Devices** table.

> **Note:**
>
> Serial number information is pulled from a physical device through SNMP. Virtual devices return a value of **N/A**.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, click on the right side of a column header.

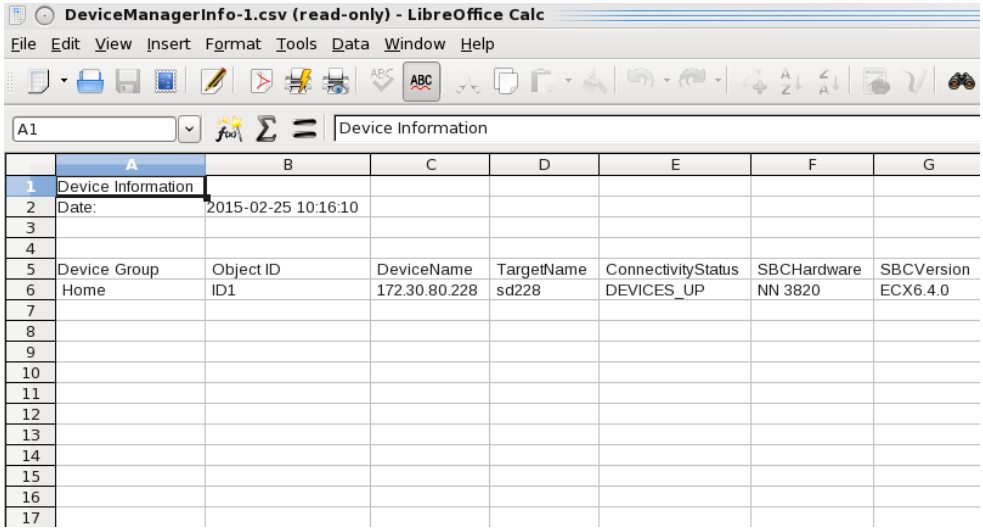
   The arrow icon appears with a drop-down menu.
3. Mouse over the **Columns** selection and click and the column options that you want to enable:
   - **Primary Serial Num**—Enables the Primary Serial Number column in the **Managed Devices** table.
   - **Secondary Serial Num**—Enables the Secondary Serial Number column in the **Managed Devices** table.

Export Device Information to Your Local System

You can export device information to your local system (PC, server, and so on) in a CSV file for auditing or device management purposes.

1. Expand the **Device Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select a device and click **Save to file**.
3. In the Web browser **Save File** dialog box, complete the fields to download the information to your system.

Figure 2-2 CSV file with device information



	A	B	C	D	E	F	G
1	Device Information						
2	Date:	2015-02-25 10:16:10					
3							
4							
5	Device Group	Object ID	DeviceName	TargetName	ConnectivityStatus	SBCHardware	SBCVersion
6	Home	ID1	172.30.80.228	sd228	DEVICES_UP	NN 3820	ECX6.4.0
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							

Note:

The columns and rows for the exported CSV file correspond to the values displayed in the **Managed Devices** pane.

Configure Device Clusters

A device cluster is a collection of devices sharing the same hardware, software, and offline configuration. The offline configuration allows members in a device cluster to share the same software version and device credentials. Device-specific parameters in the offline configuration can be targeted as data variables to set different values for each member. Once the offline configuration is specified and devices are added to a device cluster, Oracle Communications Session Element Manager can synchronize any configuration changes across all members of the cluster. You must create an offline configuration before you create a device cluster. See the *Using Offline Configurations* section in the Configuration Manager chapter for more information.

Add a Device Cluster

1. Expand the **Device Manager** slider and select **Device clusters**.
2. In the **Device Clusters** pane, click **Add**.
3. In the **Add device cluster** dialog box, complete the following fields:

Name	Description
Device cluster name field	The name for the device cluster.
Description field	The device cluster description.
Offline configuration name drop-down list	Select an offline configuration from the drop-down menu. The list populates with any existing offline configurations that you configured in the Oracle Communications Session Element Manager.

Name	Description
Hardware version field	This field is populated with the hardware product version when you select an offline configuration.
Software version field	This field is populated with the software product version when you select an offline configuration.

Add a Device to a Device Cluster

Pre-requisites: You must first add a device cluster before adding a device to a device cluster.

> **Note:**
>
> You cannot add devices to a pre-existing device cluster that was created by Oracle Communications Application Orchestrator using this task.

1. Expand the **Device Manager** slider and select **Devices**.
2. Click the **Select View** drop-down list and select **Cluster View**.
3. In the **Managed Devices - Cluster View** table, select an existing device cluster and click **Add**.
4. In the **Managed Devices - Cluster View** table, complete the following fields:

Name	Description
Configuration name field	The name of the offline configuration that the device cluster uses.
IP address 1 field	The IP address for this device.
IP address 2 drop-down list	The secondary IP address for the device. This field is required because this device is part of a cluster.
User name field	The user name for the device login account.
Password field	The password for the device login account.
SNMP community name	The name of the SNMP community.
SNMP port	The default port is 161 for SNMP traffic. Enter a different SNMP port number if you want.
Device cluster name	The name of the device cluster.
Device group	Click the ellipsis (**...**) button. In the **Set Device Group** dialog box, select the device group to which you want this device to belong. The device group now displays in the field.

5. Click **Check device** to test credentials on the target device.
6. If the device is successfully added to the device cluster, click **Next** to configure any data variables for this device.
7. In the **Configure data variable** <*offline configuration*> pane you can view the data variable provided by the device offline configuration. Click the ellipsis (**...**) button next to the data variable to view information about the data variable and its associated configuration instances.
8. Click **Finish**.

Device Cluster Management

Once you have added a device cluster, you can manage your cluster and the devices in that cluster.

View Devices in a Cluster

1. Expand the **Device Manager** slider and select **Devices**.
2. Click the **Select View** drop-down list and select **Cluster View**.
3. In the **Managed Devices - Cluster View** table, select an existing device cluster and click **Show details**.

   The **Device details** pane displays the **Hardware**, **Software**, and **License** tabs. See the *View Device Information* section for table column descriptions.

Edit a Device Cluster

1. Expand the **Device Manager** slider and select **Device clusters**.
2. In the **Device Clusters** pane, click **Edit**.
3. In the **Edit device cluster** dialog box, you can edit the description of your device cluster only:

Name	Description
Device cluster name field	The name for the device cluster.
Description field	The device cluster description. If the device cluster description can appear by default if it was created by Oracle Communications Application Orchestrator.

Delete a Device Cluster

Pre-requisites: You must delete any devices from the device cluster before you delete the device cluster.

> **Note:**
>
> If the device cluster was created by Oracle Communications Application Orchestrator, the device cluster cannot be deleted manually in this task.

1. Expand the **Device Manager** slider and select **Device clusters**.
2. In the **Device Clusters** pane, select an existing device cluster and click **Delete**.
3. In the **Delete** confirmation dialog box, click Yes to delete the device cluster.

   The device cluster is removed from the **Device Clusters** table.

Device Cluster Administrative Tasks

Once you have added a device cluster, you can manage devices in the cluster.

1. Expand the **Device Manager** slider and select **Devices**.
2. Click the **Select View** drop-down list and select **Cluster View**.
3. In the **Managed Devices - Cluster View** table, select the device cluster folder and click the **Admin** drop-down list to use the following parameter options:

Name	Description
Reboot	Select to reboot all devices in the cluster.
Synchronize alarms	Select to synchronize all alarms for all devices in the cluster.
Override lock	Select to override the lock on a device cluster or a single device in the device cluster.

3
Configuration Manager

Use the Configuration Manager navigation bar slider in Oracle Communications Session Element Manager to load, configure, apply, and save a configuration on your device.

Configuration Manager Views

The Configuration Manager has a **Default**, **ACLI**, and **List** view that lets you navigate the top-level configuration elements for your device by selecting the configuration element and its associated attributes (or parameters) in the display pane.

In the **CLI view** and **List view**, you can see more element attribute columns by checking the **Retrieve all attributes** check box. Next, when you select the column arrow menu to access element attribute column selections, all display. See the *Customize the Display* section in the Overview chapter for more information.

> **Note:**
>
> If the **Retrieve all attributes** check box is checked, it stays checked for the duration of the session.

Navigate Between Configuration Views

You can switch between views at any time during your session. When you do, the pane displays the top-level element in which you were working from the previous view. For example, if you were working in the **Default** view, under **Global settings** > **Media manager**, and you switched to the **ACLI** view, the pane displays the top-level element, **Media-manager**.

> **Note:**
>
> The column width and table pagination of the element view persist throughout the session or until the browser window is resized.

Default View

When you expand the **Configuration Manager** navigation bar slider, the **Default view** drop-down list displays by default. In this view, the top-level configuration elements are grouped logically, according to the type of configuration required. Configuration category folders are used to view top-level elements for each category. These folders display corresponding attributes (or parameters) by using Oracle Communications Session Delivery Manager labels, instead of ACLI parameter names. For example, **Proxy IP port**, is used instead of **home-proxy-port**.

The default view provides a level of organization not available with the other two views. The logical grouping of top-level elements into function-specific categories allows you to approach your configuration tasks holistically, rather than just navigating to a top-level element individually. The following table displays the categories and their sub-categories. Top-level elements are found within these categories.

Configuration Category	Sub-category	Category within Sub-Category
Global Settings	**Management** **IWF** **Security**	**IKE**
Routing	None	None
Services	**Media** **Signaling** **Agents**	**SIP**, **Translation**, **Call Admission Control**

ACLI View

The ACLI view displays top-level elements as they appear in the ACLI that is grouped under **media-manager**, **session-router**, **system**, or **security**. The ACLI view renders the configuration navigation tree in the folder that is currently active only. For example, if the configuration is loaded from a device in the devices table, the ACLI view modifies the configuration tree of this folder.

Oracle Communications Session Element Manager configuration labels are listed according to their corresponding ACLI parameter names (for example, **home-proxy-port**, and not **Proxy IP port**).

List View

The List view displays the top-level elements in an alphabetically-ordered list, in an ACLI parameter format. For example, **enum-config** is used instead of **ENUM**. There is no special grouping as with the other two views.

Enable Hidden Columns

You can enable optional hidden table columns in Oracle Communications Session Element manager so the system can collect more device attributes.

1. Glide your mouse over a column and click the drop-down list that appears next to any column heading.
2. Click the down arrow to display the menu.
3. Click **Sort Ascending** to sort the data in ascending order, or click **Sort Descending** to sort the data in descending order.
4. Click **Columns** sub-drop-down list to access a list of column names to edit.
5. Check a marked check box next to a column to hide it, or click an empty check box next to a column to display it.

Device Configuration

The **Configuration Manager** slider provides several features shown in the table below that allow you to manage the configuration of a device:

Name	Description
Devices parameter	Displays the **Managed Devices** pane where you can add devices, configure network parameters and associate them with a device group.
Device Group parameter	Displays the **Device Group** pane where you can add groups for the devices that you add.
Device Clusters folder	Displays the **Device Clusters** pane where you can add a device cluster and apply its offline configuration, and hardware and software version. This folder also contains the **Purge Policy** parameter that displays the Purge Policies pane where you can select the number of days until the user logs are purged from the system.
Software upgrade folder	From this folder menu, you can click the **Software image archive** parameter to browse to a software image on your system to upload to the archive. You can also click the **Work order administration** parameter to add a work order to a device, which includes time, policy, operational timeout and workflow parameters.

Associate Devices with Session Element Manager

The following steps are used to assign targeted devices in Configuration Manager so that Session Element Manager can manage and provide **fault, configuration, accounting, performance, security** (FCAPS) support for devices that are entered into Device Manager (which Session Element Manager shares with other applications). Once the device is assigned, Session Element Manager starts polling the device for health statistics and allows configurations to be loaded and managed for the device.

1. Expand the **Configuration Manager** slider, choose **Devices**.
2. In the **Managed Devices** table pane, click **Add devices**. The devices associated with the Oracle Communications Session Element Manager license appears in the **Devices** pane.
3. From the **Device** list, expand your device group folder and click the device you want to associate.

   > **Note:**
   >
   > You can also select a device group and have all devices in that group assigned.

4. Click **Add** to move your device to the **Devices associated with Element Management** table.
5. Click **OK**.
6. In the success dialog box, click **OK**.

   Your device is now associated with your Oracle Communications Session Element Manager so that you can load your device configuration. Repeat these steps to associate more devices to Oracle Communications Session Element Manager.

Load the Configuration of a Local Device to Configure the Device

A copy of the configuration on the device is loaded on the Oracle Communications Session Element Manager database so that this configuration can be viewed, modified, and validated with minimal interaction with the devices. You must load the configuration to view the configuration and expand it in the navigation tree. Once the configuration is loaded, you can check if the configuration copy in the database is current with the configuration version of the device. If the configuration version is not current, Oracle Communications Session Element Manager retrieves the latest configuration from the device. This on-demand loading of a configuration ensures that the local copy of the configuration and the configuration on the device are always synchronized.

1. Expand the **Configuration Manager** slider and choose **Devices**.
2. In the **Devices** table, click the arrow next to the device group folder to expand the list of devices within this device group.
3. Click the device you want to load and click **Load**.
4. In the success dialog box, click **OK**.

   The device's configuration is loaded and appears as a heading above the **Devices** table.

Load a Configuration Schema for a Device

All device software release configuration information is modeled and maintained in a configuration schema. A device needs to have a valid configuration schema in to be managed by Oracle Communications Session Element Manager. If a device schema does not exist for a device software release, the device is considered to be not manageable. A device that cannot be managed can be added to Device Manager, but it cannot be assigned to Configuration Manager. Loading a configuration schema for the software release of a device is required only if the device software release does not come with the XSD configuration file (also referred to as the XSD model) already embedded in the image.

Oracle Communications Session Element Manager searches for a valid model XSD configuration file in the database local schema repository first. If it is not found, Oracle Communications Session Element Manager attempts to get the XSD configuration file directly from the device (in recent device releases, the XSD configuration file is packaged with the release image), and put it in the database local schema repository. This process is hidden from the user.

If Oracle Communications Session Element Manager is unable to get the XSD file from the device, you must use the load configuration schema tool described in the following section to upload the XSD configuration file.

> **Note:**
>
> If the release version of your device does not match or is not supported in your version of Oracle Communications Session Element Manager, new configuration elements can continue to be configured from the Configuration Manager **Devices** table with either the **ACLI** or **List** view.

Upload a Configuration Schema for a Device

1. On the menu bar, choose **Tools** > **Upload configuration schema file**.
2. In the **Upload configuration schema file** dialog box, click **Browse** and navigate to a valid .xsd configuration file.
3. In the dialog box, choose the configuration schema you want to upload and click **Open**.
4. Click **Upload** to start the upload process.
5. In the success dialog box, click **OK**.

Manage Device Configurations

You can configure devices for session delivery products in the GUI. Most of these functions can also be configured in the ACLI and both configuration access methods can be used simultaneously.

Use the actions below to manage loaded device configurations in the **Managed Devices** pane for top-level device management functions.

Name	Description
Refresh	Click to refresh all devices for all device groups listed. This action is always enabled.
Expand All	Click to expand the folder of devices in the home directory on the **Managed Devices** pane.
Collapse All	Click to collapse the folder of devices in the home directory on the **Managed Devices** pane.
Select View	Click to select either the group view or cluster view of devices in the home directory on the **Managed Devices** pane.
Add	Click to select a device group or device and associate it with Oracle Communications Session Element Manager.
Save to file	Click to save the device or device group configuration to your system.

Use the actions below to manage loaded device configurations in the **Managed Devices** pane to do actions on a device.

Name	Description
Load	Click to load a selected device's configuration so that it can be edited.

> **Note:**
>
> If a new configuration version is available, the corresponding device's configuration data.

Name	Description
View Changes	Click to display a list of all configuration changes for the selected device. By default, the table initially displays the changes made by the current user. **Note:** If you change the **User** parameter to another user, or to the **all** value, you can view all users' changes in a single list. If you have the appropriate user privileges, you can do the following actions in the Configuration changes dialog box: **Note:** You cannot undo, change, or update the changes made by another user. • **Refresh**—Click to refresh the data in the view changes list. • **Undo Changes**—Click to undo all changes you made to this device. • **Change Owner**—Click to transfer the ownership of your changes to another user. • **Update**—Click to launch a dialog box that is used to update the configuration with one of the following options: – **Save & activate configuration**—(Default) Choose to save the configuration and make the current configuration on the device the running configuration. – **Save configuration**—Click to save the current configuration changes to the device. – **Activate configuration**—Click to make the current configuration the running configuration. • **Save to file**—Click to display data to a text file in comma separated values (CSV) format.

Name	Description
Update	**Update**—Click to launch a dialog box that is used to update the configuration with one of the following options: • **Save & activate configuration**—(Default) Choose to save the configuration and make the current configuration on the device the running configuration. • **Save configuration**—Click to save the current configuration changes to the device. • **Activate configuration**—Click to make the current configuration the running configuration. **Note:** The first two options are only available if ther are pending changes to be saved. The third option is only available if there are no user changes, and there is a saved configuration pending activation.
View tasks	Click to view the device tasks (or operations) performed on this device.
Get Inventory	Click to access configuration inventory details for this device.
Select View	Click to choose either the group view or cluster view of devices in the home directory on the **Managed Devices** pane.

View Device Data

The following **Managed Devices** table columns for loaded devices, is described below:

Data	Description
Device	The device (or HA pair) in the device group.
Target Name	The user-defined name of a device.
Software Version	The full release version, including patch number, of software on the device.
Hardware Version	The full hardware platform identification.
Group/Cluster	The device group or device cluster to which the device belongs.
SBI TLS Status	(Hidden) The status of the south bound interface (SBI) transport layer security (TLS) configuration for session delivery network functions like MSG that supports ACP over TLS.
Primary Serial Num	(Hidden) The primary serial number of the device.
Secondary Serial Num	(Hidden) The secondary serial number of the device.
Object ID	(Hidden) The SNMP object ID assigned to the device.

Remove Device Data

A device can be removed from Oracle Communications Session Element Manager by removing its association with the Oracle Communications Session Element Manager license.

1. Expand the **Configuration Manager** slider and click **Devices**.
2. In the **Managed Devices** table, click **Add devices**.

3. In the **Devices associated with Element Management license** pane, expand the device group folder in the **Total associated device count** panel and click the device you want to remove.
4. Click **Remove**.

   Your device is no longer associated with Oracle Communications Session Element Manager and appears in the **Device List** pane.
5. Click **OK** to apply the changes.

Use Offline Configurations

An offline configuration is a common, top-level configuration template that is used to provision one or more devices without having to target each device and its elements with specific values. An offline configuration can be created by making a copy of an existing configuration, packaged configuration, managed device configuration, or by selecting a schema from a supported software model. When you copy an existing configuration, data variables allow network administrators to target elements that require device-specific information. All data variables must have new values to push the configuration to a device.

Use Pre-existing Offline Configuration Templates

Several packaged offline configurations are included with Oracle Communications Session Element Manager for Oracle Communications Session Delivery Products. Each offered offline configuration template contains a base configuration for specific types of network environments. Below is a the list of base offline configuration templates that are available.

Consider the following before you create your offline configuration:

- Know all data variables (DV) that identify individual device-specific parameters that are required for each device that the offline configuration supports.
- Create a detailed network topology map, including network domain information (slots, ports and networks, realms, and their relationships to each other).
- Change any applicable physical configuration settings to match the offline configuration that you are going to create.

The following table describes the pre-existing packaged offline configuration templates for you to copy and use for different network application types.

> **Note:**
>
> Oracle Communications recommends that you make a copy of the applicable packaged offline configuration template itself for your own offline configuration so that you can continue to reuse this template for other domains that you may want to create. After an offline configuration is associated with a cluster of devices, it is no longer available for other devices or clusters.

Packaged Offline Configuration	Network Application
SLRM_Standalone	• Access-hybrid IMS Oracle Communications Session Routers (SRs) with subscriber-aware load balancing and route management (SLRM) systems, and Oracle Communications Session Border Controllers, and physical session routers (IMS Access Hybrid). • SLRMs only. • Core IP multi-media Subsystem (IMS) Oracle Communications Session Routers and SLRMs (IMS Core).
CSM_HA	• High-availability (HA) IMS Core • HA IMS Access Hybrid
CSM_Standalone_SlrmLink	Standalone Oracle Communications Core Session Manager (CSM) that is configured to work with an SLRM.
CSM_HA_SlrmLink	An HA CSM that is configured to work with an SLRM.
ASBC_Standalone_SlbSlrmLinks	• Access standalone Oracle Communications Session Border Controllers (SBCs) • Subscriber-Aware Load Balancers (SLBs) • SLRMs • IMS Access Hybrid
ASBC_HA	Access SBCs for HA 3G to 4G mobile phone network.
SR_Standalone	Standalone SBCs.
SR_HA	Standalone HA SRs.
ASBC_HA_SlbSlrmLinks	Access SBCs for high-availability 3G to 4G mobile phone network with SLBs and SLRMs.
SLB_Standalone	• Standalone SLBs • IMS-Access-Hybrid

Copy an Offline Configuration Template

Use this task to copy an existing configuration or packaged offline configuration template to make a new offline configuration for your specific domain.

1. Expand the **Configuration Manager** slider and select **Configuration tools** > **Offline configurations**.
2. In the **Offline Config** tab, select an offline configuration template from the table and click **Copy**.
3. In the **Copy Offline Configuration** dialog box, enter the name of the new offline configuration.
4. In the **Success** dialog box, click **OK**.

   The new offline configuration appears in the table.

Load your new offline configuration. Your new offline configuration is populated with a base set of parameter values that you can modify to configure your domain.

Create an Offline Configuration

A configuration can be seeded from a supported software version schema or from an existing managed device configuration.

1. On the **Configuration Manager** slider, choose **Configuration tools** > **Offline configurations**.
2. In the **Offline Config** tab, click **Add**.
3. In the **Offline Configuration** pane, complete the following fields:

Name	Description
Configuration name field	The unique name for the configuration.
Description field	The description for the configuration.
Offline configuration seeded from drop-down list	Choose from the following methods to create the configuration: • **Software version**—Choose to create an offline configuration from a supported software version schema. • **Managed Device**—Choose to create an offline configuration by copying an existing managed device configuration.
Platform drop-down list	(Available with the **Software version** parameter) Choose the device hardware version to seed the configuration from a device template.
Supported software version drop-down list	(Available with the **Software version** parameter) Choose the device software version in order to seed the configuration from a device template.
Selected managed device field	(Available with the **Managed Device** parameter) Click the ellipsis (...) to launch the **Select managed device** dialog box to navigate to a device associated with Oracle Communications Session Element Manager and click **OK**. This field populates with the IP address of the device.

4. Click **Apply**.
5. In the **Success** dialog box, click **OK**.

Load your new offline configuration. Your new offline configuration is populated with a base set of parameter values that you can modify to configure your domain.

Load an Offline Configuration

Use this task to configure, modify, or edit parameters for your offline configuration for your system domain.

1. On the **Configuration Manager** slider, choose **Configuration tools** > **Offline configurations**.
2. In the **Offline Config** tab, choose the offline configuration that you want to use from the table and click **Load**.
3. In the **Success** dialog box, click **OK**.

   The configuration navigation tree is expanded under the **Offline Configurations** folder in the navigation pane. You can use this navigation tree to get to the required configuration elements.
4. Navigate the offline configuration and configure, modify or edit parameters in your offline configuration.

Create Data Variables to Support Device Specific Values

An offline configuration can require data variables (DVs) that can have different values for each device that the template is assigned to support. This allows the template to be finely adjusted to the specific needs of a device and continue to provide a common baseline configuration for many devices. The template editor allows the user to apply data variables to any element attribute that is supported in the offline configuration. A derived value can be specified in cases where the DV that you are configuring shares the same value as another DV (dependency).

1. On the **Configuration Manager** slider, choose **Configuration tools** > **Offline configurations**.
2. In the **Offline Config** tab, choose the offline configuration that you want to use from the table and click **Load**.
3. In the **Success** dialog box, click **OK**.

   The selected offline configuration appears under **Offline Configurations** folder.
4. Navigate to any configuration element in the navigation tree.
5. When element attributes are rendered, click the DV tool icon  in the upper right of the configuration body panel and select an attribute to apply a data variable. A dialogue box appears if the targeted attribute supports DVs. The following table describes the required entries:

Name	Description
Selecting existing DV drop-down list	This list is populated if previous data variables where created. This feature allows the use of DVs that share the same values across different elements such as an IP address. You can select an existing DV for re-use so that all fields are populated. If you are creating a new DV, keep the blank selection and enter a new entry by filling out other fields in this table. Select an existing DV to pre-populate the following parameters.
Name field	The an unique ID for the data variable. For example: **WANCOM2_UTIL_ADDR**
Label field	The name for the DV that appears in the individual VM configuration wizard.
Description field	The description for the DV that appears in the tool-tip during configuration.
Default value field	The default value for the DV.

> **Note:**
>
> This value can be overwritten when you apply a template to a device.

Name	Description
Derive value check box	This box is not checked by default. Check the check box to make the **Formula** field appear so that the value for this DV is derived from the source information in the formula. **Note:** Unchecking this box makes the **Formula** field disappear.
Formula field	The formula contains the name of the DV (in brackets) that is being referenced by this DV. For example: ${WANCOM2_UTIL_IP}. In this example, the WANCOM2_UTIL_IP DV is being referenced by the WANCOM2_UTIL_ADDR.

6. Click **Add**.
7. Click **Apply** to submit configuration changes.
8. In the **Success** dialog box, click **OK**.

Apply an Offline Configuration

In Oracle Communications Session Element Manager, an offline configuration has defined data-binding variables, which are applied to allow members in a device cluster to share the same software version and device credentials. See the *Configure Device Clusters* section in the High Availability chapter of the *Oracle Communications Session Delivery Manager Administration Guide* for more information.

In Oracle Communications Application Orchestrator, the offline configuration is associated with a deployment unit (DU) to configure device-specific parameters for the VM device(s) associated with this DU and with the Hierarchical Service Configuration (HSC) feature. See the *Configure Device Specific Parameters for a DU* section in the Operationalize a CNF Manually chapter and the Build the Hierarchical Service Configuration chapter of the *Oracle Communications Application Orchestrator User Guide* for more information.

Configure and Apply Reusable Configuration Modules

Reusable Configuration Modules (RCMs) are work flow templates that describe a sequence of configuration changes that can be used to deploy features. Some examples are adding a session agent to a session agent group, adding a new trunk service, etc. The modules are designed around the configuration of a particular functionality for the specified device configuration elements. By targeting specific attributes, RCM can be applied without having to modify the top-level elements. A clustered environment is not required and modules are not tied to a specific software version.

When you apply an RCM to a target configuration, Oracle Communications Session Element Manager validates that the designated attributes are supported by the target configurations platform and software release version.

Access and Manage RCMs

The following actions are available to access and manage all custom and packaged RCMs in the **Reusable Configuration module** table.

Name	Description
Refresh button	Click to refresh the table contents.
Log button	Click to show user visible logs for the selected RCM.
Add button	Click to create a new RCM.
Edit button	Click to edit the current RCM elements.
Apply button	Click to apply the RCM to a target configuration. The user is prompted for input values.
Manage > **Modify definition** button	Select to modify the RCM properties.
Manage > Copy button	Select to create a new RCM using a copy of the selected RCM.
Delete button	Click to delete the selected RCM.

Packaged RCM

This release includes a number of packaged reusable configuration modules that contain a pre-configured workflow.

The following table describes the packaged RCMs that come with Oracle Communications Session Delivery Manager:

Name	Description
rcmAddSBCtoSR	Adds an Oracle Communications Session Border Controller to an Oracle Communication Session Router configuration.
rcmAddSLRMtoCSM	Registers an Oracle Communications SLRM with an Oracle Communications Core Session Manager configuration.
rcmRemoveSLRMfromASBC	Removes an Oracle Communications SLRM from an Oracle Communications ASBC configuration.
rcmRemoveSLRMfromCSM	Removes an Oracle Communications SLRM from an Oracle Communications Core Session Manager configuration.
rcmRemoveSLBfromSBC	Removes an Oracle Communications Subscriber-Aware Load Balancer from an Oracle Communications Session Border Controller configuration.
rcmAddSLBtoSBC	Adds an Oracle Communications Subscriber-Aware Load Balancer to an Oracle Communications Session Border Controller configuration.
rcmAddSLRMtoASBC	Adds an Oracle Communications SLRM to an Oracle Communications ASBC configuration.
rcmRemoveSBCfromSR	Removes an Oracle Communications Session Border Controller from an Oracle Communications Session Router configuration.

User Roles

- **RCM Designer** — The designer creates reusable configuration modules from existing device schema models. A good understanding of the data model schema and device configuration is required, due to the element hierarchy and element dependency rules.

  > **Note:**
  >
  > RCM can be applied to any Oracle Communications Session Delivery Manager supported software model.

  The following actions apply to the designer:

  1. Create a RCM from a Schema
  2. Load a RCM
  3. Delete a RCM
  4. Add an Element
  5. Modify Element Properties
  6. Delete an Element
  7. Define Element Attribute Values

- **End User** — End users associate an RCM with device configurations by inputting values for the specified variables. This abstracts the end user from the model schema, allowing for the configuration of specific functionality without knowledge of the element topology. Oracle Communications Session Delivery Manager modifies specified attributes in the target configuration to the values contained within the RCM

  The following actions apply to the end user:

  1. Apply RCM to Target Device Configuration
  2. Apply RCM to Target Global Configuration
  3. Configure RCM Input Values

Enter RCM Input Values for a Device

The following options are used to input values when applying an RCM to a device:

- **Define Element Attribute Values**— Designers can pre-configure attribute values for elements contained within a RCM. See *Define Element Attribute Values* for information on this task.
- **Wizard** — The wizard prompts the end user for all specified input variable values. Each page displays a maximum of 10 variables and not all may belong to the same element. If an input variable applies to more than one attribute in the same or a different element, there is only a single prompt for that value.

  > **Note:**
  >
  > The wizard does not save any input data into persistent database until the user clicks the **Apply** button.

- **NM** — Input values are passed to RCM through packaged composite network functions (CNFs) using the notification message (NM) system. This is an automatic process for devices managed through Oracle Communications Application Orchestrator using canned CNFs and requires no additional configuration.

Provisioning Policy Rules for RCM Actions

Use the following rules for RCM actions for each element instance level (for example, top level element, sub-element, etc):

- An **ADD** element may not contain any sub-element with a **MODIFY** or **DELETE** action.
- A **MODIFY** action cannot be performed on the parent of any configuration element that is part of an Order Group.
- Required sub-elements cannot be removed from RCM elements with a top level **ADD** action.
- A **MODIFY** or **DELETE** top-level element can only change into an **ADD** action if all it's required sub-elements exist.

Create a RCM from a Schema

To provision a new RCM from an existing software model schema:

1. Expand the Configuration Manager slider and navigate to **Configuration Tools** > **Reusable Modules**.
2. Click **Add**.

Name	Description
Namefield	Enter a unique name for the RCM.
Description field	Enter a description for the RCM.
Modifiable drop-down list	Select the permissions for users to modify this RCM: • **public**—Any user can modify this RCM. • **private**—Only the creator can modify this RCM.
Platform drop-down list	Select the platform of the device software that the RCM is based on.
Supported software version drop-down list	Select the device software version that the RCM is based on.

3. Click **Apply**.

Add an Element to an Existing RCM

To add an element to an existing RCM:

> **Note:**
>
> You must load the target RCM before editing the configuration data.

1. Select the RCM you want to modify listed under **Configuration Manager** slider and select **Configuration Tools** > **Reusable Modules**.
2. Click **Add**.

Name	Description
Type drop-down list	Select the type of element to be defined
Name field	Enter a unique name for the element action.
Description field	Enter a description for the element action.
Element action drop-down list	Select the permissions for users to modify this RCM: • **ADD**—Adds the selected element if it is not found in the target work flow. • **MODIFY**—Modifies the selected element if found in the target work flow. • **DELETE**—Deletes the selected element if found in the target work flow.

3. Click **Add Variable**.
4. Click **OK** to dismiss the confirmation dialog.

Modify Element Properties in an Existing RCM

To modify an element in an existing RCM:

> **Note:**
>
> You must load the target RCM before editing the configuration data.

1. Select the RCM you want to modify listed under **Configuration Tools** > **Reusable Modules**.
2. Select the element you want to edit in the **Elements defined** table and click **Edit**.
3. Select the element you want to edit in the **Elements defined** table and click **Modify definition**.

Name	Description
Description field	Enter a description for the.
Element action drop-down list	Select the permissions for users to modify this RCM: • **ADD**—Adds the selected element if it is not found in the target work flow. • **MODIFY**—Modifies the selected element if found in the target work flow. • **DELETE**—Deletes the selected element if found in the target work flow.

4. Click **Apply.**.
5. Click **OK** to dismiss the confirmation dialog.

Pre-Define Variable Values for an Element in an RCM

To pre-define the variable values for an element in an RCM:

> **Note:**
>
> You must load the target RCM before editing the configuration data.

1. Expand the **Configuration Manager** slider and select **Configuration Tools** > **Reusable Modules** and select the RCM that you want to modify.
2. Select the element you want to edit from the **Elements defined** table and click **Edit**.
3. Select the element you want to edit from the **Elements defined** table and click **Edit**.
4. **Attribute name**—Enter a pre-defined input value.
5. Repeat until all required variables are defined.
6. Click **Apply**.
7. Click **OK** to dismiss the confirmation dialog.

Apply an RCM to a Device

1. Expand the **Configuration Manager** slider, and select **Configuration Tools** > **Reusable Modules**.
2. Select the RCM that you want to apply to a device, and click **Apply**.
3. In the **Apply RCM to configuration** pane that appears, select the ellipse icon (**...**) next to the **Select managed device** field.
4. In the **Select managed device** dialog box, navigate the desired folder structure to your device.
5. Select the device, and click **OK**.
6. In the **Apply RCM to configuration** pane, click **Next**.
7. In the Configure **RCM input variables** pane, configure the input parameters for your device and click **Finish** when you are done.

Manage a Reusable Configuration Module

Load an RCM

You must load an RCM to view or edit the contents. To load an RCM work flow from the Reusable Configuration Module table:

1. Expand the **Configuration Manager** slider and select **Configuration Tools** > **Reusable Modules**.
2. Select an RCM and click **Load**.

View Reusable Configuration Modules

1. Expand the **Configuration Manager** slider, and select **Configuration Tools** > **Reusable Modules**.
2. View the following **Reusable Configuration module** table columns for the listed RCM entries:

Name	Description
Name	The RCM name.
Description	The RCM description.
Last modified date	The date and time when the RCM was last changed.
DNM	Dependancy notification message (DNM). **Note:** This column is not used.
Created data	(Hidden) The date at which data was created for this RCM.
Created by	(Hidden) Indicates user who created the RCM. A preexisting RCM indicates **EM_SYSTEM**.
Category	(Hidden) The product plugin vendor category. For example, **SD** (Session Delivery).
Component	(Hidden) The element manager (EM) plugin product NF component. **Note:** This field populates with **Default** when the SD product plugin vendor category is selected.
Schema version	(Hidden) The software model schema for devices.
Modifiable	(Hidden) Indicates the following permisions: • **public**— Any user can modify this RCM. • **private**—Only the creator of the RCM can modify this RCM.

Update a Device Configuration

1. Expand the **Configuration Manager** slider and choose **Devices**.
2. Select the device you wish to modify from the **Managed Devices** table.
3. Select the Update button and
   - **Save & activate configuration**—(Default) Choose to save the configuration

     and make the current working configuration on the device the running configuration.
   - **Save configuration**—Click to save the current working configuration changes to the

device.

- **Activate configuration**—Click to make the current working configuration the running configuration.

Delete an Element from an Existing RCM

To delete an element from an existing RCM:

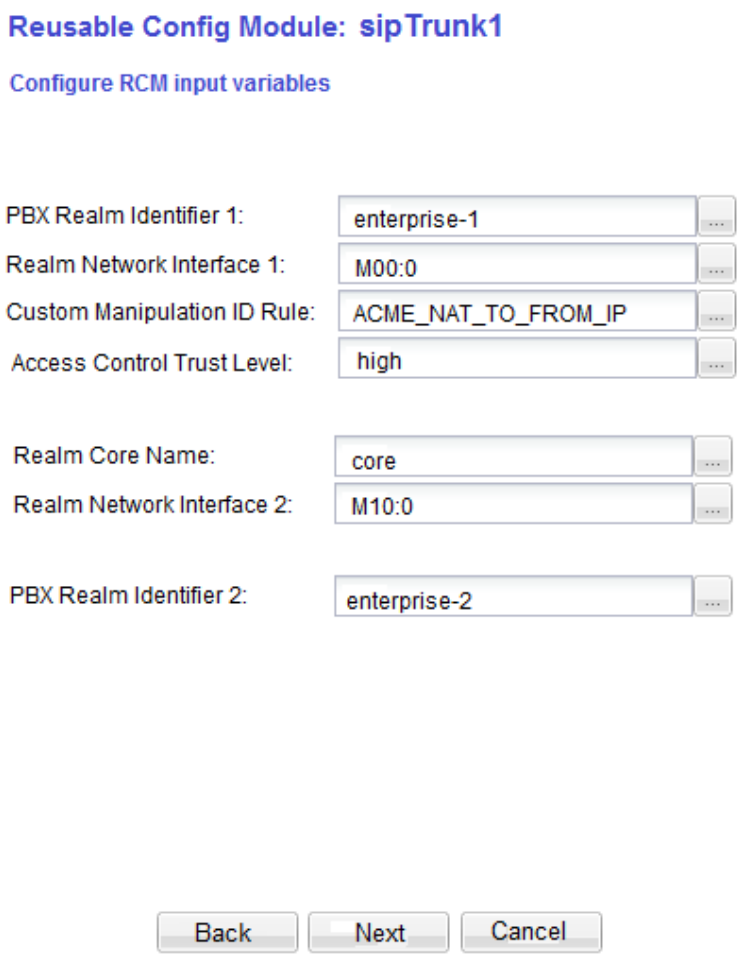
> **Note:**
>
> You must load the target RCM before editing the configuration data.

1. Expand the **Configuration Manager** slider and select **Configuration Tools** > **Reusable Modules** and select the RCM that you want to modify.
2. Select the element you want to edit from the **Elements defined** table and click **Delete**.
3. Click **OK** to dismiss the confirmation dialog.

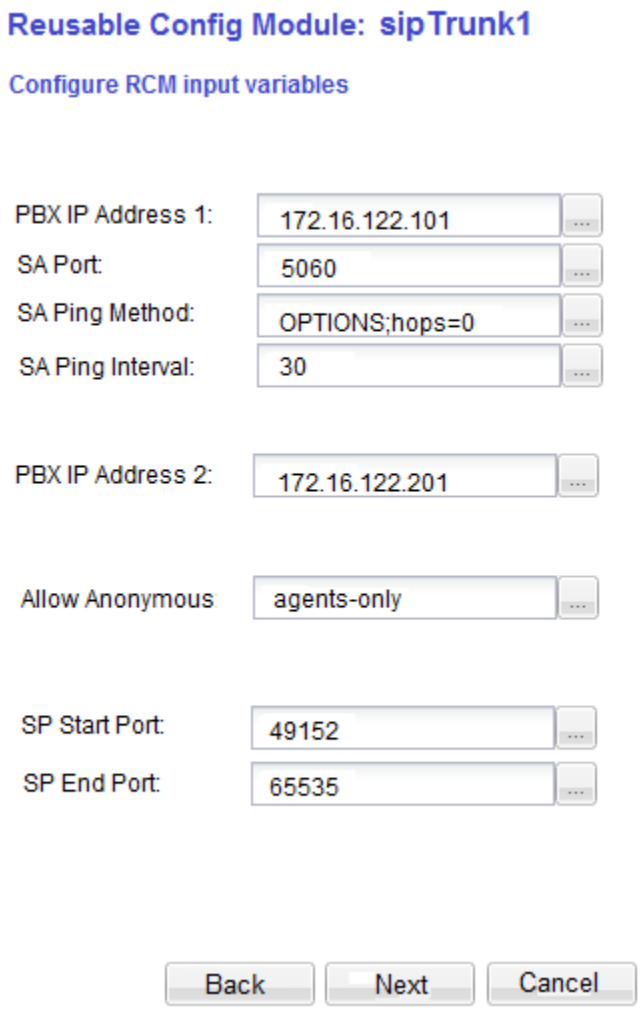
Configure RCM Input Values

The following example runs through the process of an end user entering input values with the **RCM Input wizard** screen for a SIP Trunk service RCM. This example of the wizard has 3 pages.

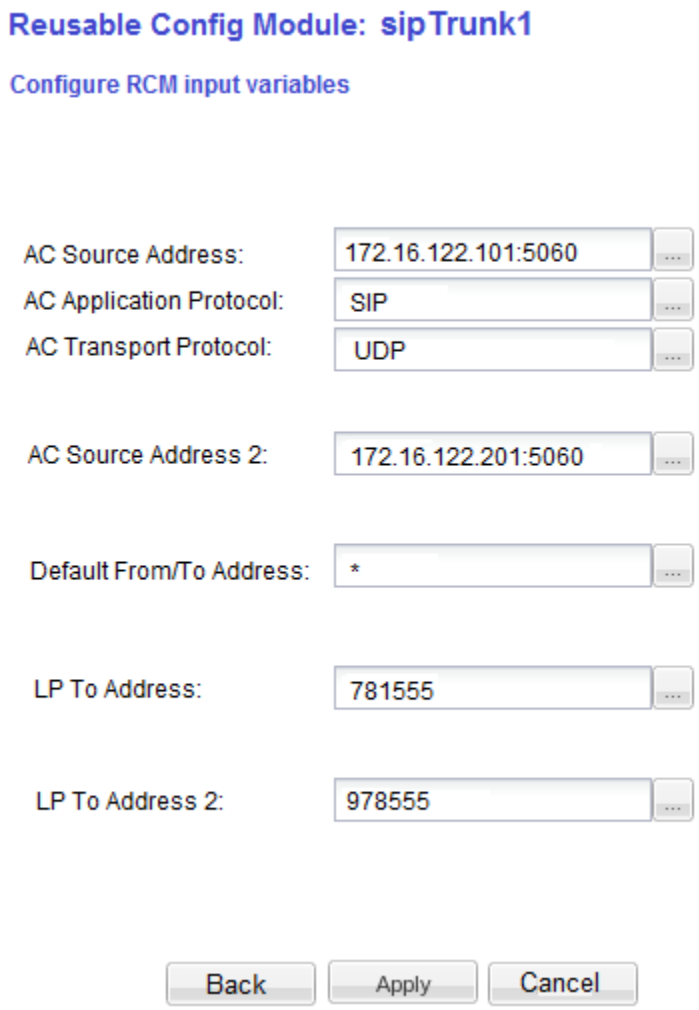
1. Enter values for all specified attributes and click **Next**.



2. Enter values for all specified attributes and click **Next**.



3. Enter values for all specified attributes and click **Apply**.



The configuration modifications are validated against the target device's data model schema.

Delete an RCM

Deleting an RCM work flow permanently removes it from the database. Once deleted, it cannot be retrieved. The RCM is only deleted if it is not assigned to any device or configuration with a dependency on it. To delete an RCM from the Reusable Config Modules table:

1. Expand the **Configuration Manager** slider and select **Configuration Tools** > **Reusable Modules**.
2. Select an RCM from the Reusable Config modules table.
3. Click **Delete**.
4. Click **Yes** in the confirmation dialog box.

Manage the Configuration Archive

Depending on your user privilege level (or privileges set for the User Group to which you belong), you can manage the configuration archive. See the *Security Manager* chapter in the

Oracle Communications Session Element Manager Administration Guide if you need to change your privileges in order to manage the configuration archive.

The following sections describe the operations necessary to manage the configuration archive for devices and device groups.

> **Note:**
>
> A configuration can exist on every node of a device cluster. When a configuration file is pulled from a device by a node, the file is sent to all cluster nodes.

Add a Backup Schedule

Use this task to schedule automatic configuration backup for device(s) or a device group to run once, daily, weekly, or monthly automatically. You can also configure this backup so that it can happen on demand. The following actions occur when a backup is created:

- A new directory is created for each device using its IP address in the **AcmePacket/ConfigBackups** directory.
- An entry is added to the database for the configuration file.
- The set purge policy is applied.

1. On the **Configuration Manager** slider, select **Configure archive** > **Schedules**.
2. In the **Schedules** pane, click **Add schedule**.
3. In the **Add Schedules** tab, complete the following fields:

Name	Description
Schedule drop-down list	Select from the following options to set the type configuration backups for devices: • **Schedule**—Choose to set a date and time. • **On Demand**—Choose to make the configuration backup available on an on-demand basis. If you choose this option, the other parameters are unavailable. If you select this option, a backup can be launched whenever you want.
Frequency drop-down list	Select from the following options to set the frequency of configuration backups for devices: • **None**—Choose to not repeat a scheduled backup. • **Daily**—Choose to perform daily backups. • **Weekly**—Choose to perform weekly backups. • **Monthly**—Choose to perform monthly backups.
Start date drop-down list	Choose a start date using the calendar icon.
Start time drop-down list	Choose a start time in a 24-hour cycle.

4. Click the **Devices** tab.
5. Click **Add**.
6. In the **Select Device** dialog box, choose the device(s) or device group(s) in the **Managed devices** pane for which you want to schedule a backup and click **Add** to move them to the **Targeted devices** pane.
7. Click **OK**.

Your targeted device for scheduled configuration backups appears in the **Devices** table.

8. Click **Apply** to complete the backup schedule for your device.

Restore a Configuration Backup

The purge policy or existing configuration backups are not affected when a backup is restored for a device.

1. On the **Configuration Manager** slider, select **Configure archive** > **Archive configuration**.
2. Select a backed up configuration from the table and click **Restore**.
3. In the confirmation dialog box, click **Yes** to restore the backed-up configuration.

Rename a Configuration

You can rename any backed up configuration file to make its name more meaningful. The actual file name on the system does not change and continues to adhere to the set file naming policy. This configuration name only appears within the context of Oracle Communications Session Element Manager.

1. On the **Configuration Manager** slider, choose **Configure archive** > **Archive configuration**.
2. In the **Archive configurations** pane, choose the configuration you want to rename and click **Rename**.
3. In the **Name** field, enter a new name for the configuration.
4. Click **OK**.

   The alias name for the configuration appears in the list of archive configurations instead of its actual configuration file name.

Search for an Archive Configuration

1. On the **Configuration Manager** slider, choose **Configure archive** > **Archive configuration**.
2. In the **Configuration archive search** dialog box, use the following fields to specify your search criteria.

Name	Description
Configuration name field	Enter the name of a configuration.
Source field	Enter the target device name.
Hardware version field	Enter the platform version of a device.
Software version field	Enter the software version of a device.
Start backup date field	Choose a start time from the calendar.
End backup date field	Choose an end time from the calendar.

3. Click **OK**.

Manage Purge Policies

You can select a purge policy for devices or device groups. This policy can be customized to define the number of backup configurations to store per device, configure the purge schedule for devices or device groups, or purge them immediately.

Create a Configuration Purge Policy

A purge policy must be selected and configured to have Oracle Communications Session Element Manager automatically delete configurations. You can also manage backed up configurations manually.

The Oracle Communications Session Element Manager plugin service provides the archive configuration name prefix for the archive configuration file name. The archived configuration files are kept in the Oracle Communications Session Delivery Manager server folder name ConfigBackups under the AcmePacket directory. The archived configuration file for each device uses the device IP address in the directory path.

1. On the **Configuration Manager** slider, select **Configure archive** > **Administration**.
2. In the **Purge policy** tab, complete the following fields:

Name	Description
Configuration archive purge policy section	Choose one of the following options to purge configurations: • **Policy 1**—Total Number of back-up configurations to allowed to be stored per device. • **Policy 2**—Back-up configurations for devices are purged on a daily, weekly or monthly basis.
Policy 1 section	Enter a numerical value between 0 - 999999999.
Policy 2 section	Enter values for the following fields: • **Deleting daily backup older than days**—Enter a numerical value between 0 - 999999999. The default is 4 days. • **Deleting weekly backup older than weeks**—Enter a numerical value between 0 - 99999999. The default is 4 weeks. • **Deleting monthly backup older than months**—Enter a numerical value between 0 - 999999999. The default is 4 months.

3. Click **Apply**.

Purge Configurations On-Demand

You can select the purge policy you set earlier or target all backed up configurations on a device or group. You can select multiple devices or multiple groups to purge at one time.

1. On the **Configuration Manager** slider, choose **Configure archive** > **Administration**.
2. Click the **Operation** tab and complete the following fields:

Name	Description
Configuration archive purge policy section	Choose the scope of the purge: • **Purge all archived configuration**—Choose to purge all files and configurations associated with selected device(s) or device group(s). • **Purge per policy**—Choose to purge selected devices according to set purge policy.

3. Choose the device group folder that you want to purge and click **Add device Group**.
4. Click **Purge**.

Search the Archive for a Configuration

Use this task to search for a configuration in the configure archive for an existing configuration backup.

The following search criteria can be used:

- Standard wild card ***** and **?** characters are supported.
  - ***** matches 0 or more characters.
  - **?** matches 1 character.
- Search filters containing wild card characters must be enclosed in double quotes: **"fo*"**.
- Search filters containing no wild card characters result in an exact match.
- Wild card characters cannot be used outside of double quotation marks in combination with an exact match search.

  "A*1" is a valid search filter.

  "A*"* is not a valid search filter.

1. Expand the **Configuration Manager** slider and click to expand the **Configure archive** folder in the navigation pane.
2. Click **Archive configuration** in the navigation pane.
3. In the Archive configurations pane, click **Search**.
4. In the **Configuration archive search** dialog box, complete any of the following fields:

Name	Description
Configuration name field	The user-defined name for the device configuration.
Source field	The source IP address of the device.
Hardware version field	The hardware version of a device.
Software version field	The software version of a device.
Start backup date field	Click the calendar icon to select the start date range for when a configuration was backed up to the configuration archive.
End backup date field	Click the calendar icon to select the end date range for when a configuration was backed up to the configuration archive.

5. In the **Success** dialog box, click **OK**.

   The newly-added physical interface appears in the **Physical interface** table.

Configure Session Delivery Devices for Session Element Manager

The following sections are used to verify some basic parameters for session delivery product devices which include bootstrapping, system, SNMP, and traps and the configuration of some basic networking parameters for session delivery products. See your session delivery product device documentation for more configuration information that is beyond the scope of this guide.

Verify Session Delivery Product Configurations

The Oracle Communications Session Delivery product configurations you plan to manage using Oracle Communications Session Element Manager must have the correct system information configured to properly load into Configuration Manager. See the *Oracle Communications ACLI Reference Guide* for more information about the ACLI commands that are used in these system configurations.

Check Boot Parameters

Boot parameters specify the information that your Oracle Communications Session Delivery system uses at boot time when it prepares to run applications. You must configure the system IP address, subnetwork (subnet) mask for the management interface (wancom0), and a unique target name.

> **Note:**
>
> Do not use the default session delivery product name **acmesystem**.

Oracle Communications Session Element Manager uses the target name to uniquely identify a Oracle Communications Session Border Controller from the list of Oracle Communications Session Delivery products in the content area. You need to ensure that all Oracle Communications Session Delivery products you plan to load and manage in Oracle Communications Session Element Manager have unique target names or the entire list of Oracle Communications Session Delivery products appear with the default acmesystem name.

Check the System Configuration Element

You need to ensure the **system-config** element, which establishes that general system information and settings for the Oracle Communications session delivery product system, has been configured with the following SNMP and networking parameters:

- System contact information.
- System ID.
- Physical location of the system.
- SNMP is enabled on the system.
- Traps are enabled on the system.
- The network default gateway IP address is configured.

If you need more information about configuring these parameters, see your session delivery product configuration guide and the **Oracle Communications ACLI Reference Guide**.

Check the SNMP Community Element

The **snmp-community** element must be configured with the following parameters to specify the Oracle Communications Session Element Manager server from which the Oracle Communications Session Delivery product system accepts SNMP requests:

- Ensure that the Oracle Communications Session Element Manager server IP address is configured and the server is running.
- Ensure that the IP address(es) for SNMP communities are specified for authentication purposes. If the **snmp-community** element is configured for a cluster, you must add all the IP addresses for each member in the Oracle Communications Session Element Manager cluster.
- If you change the snmp-community values for your Oracle Communications Session Delivery product, you must remove this device from the Device Manager, and add it again so that the Oracle Communications Session Element Manager server can update this SNMP information.

Check the Trap Receiver Element

The **trap-receiver** element is configured on the Oracle Communications Session Delivery product system so that the Oracle Communications Session Element Manager server can receive SNMP traps for event reporting. Ensure that the following parameters are specified:

- The Oracle Communications Session Element Manager server IP address is specified.
- The filter level must be set to **All**.
- The community name must match the name in the SNMP community element.

> **Note:**
>
> If you configure the trap-receiver element for a cluster, you need to add all the IP addresses for each member in an Oracle Communications Session Element Manager cluster.

Add Physical Interfaces

Use Oracle Communications Session Element Manager to add a physical interface for your session delivery device.

1. Expand the **Configuration Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select a device and click **Load**.
3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.
4. In the navigation panel, click **Interfaces**.
5. In the **Interfaces** pane, click **Add** in the **Physical interface** table.
6. In the **Add Physical interface** dialog box, complete the following fields:

Name	Description
Name field	Enter a unique name for this interface using any combination of characters entered without spaces.
Operation type drop-down list	Select one of the following physical interface types: • **Maintenance**—The management physical interface that is used for management protocols or high availability (HA). • **Control**—This is a legacy parameter that can also be used to configure the management physical interface. • **Media**—The media interface which carries production traffic.
Slot field	Enter the slot of this physical interface (**0** or **1**).
Port field	From left to right as you face the chassis, the possible values are from **0** to **3**.

7. Click **Apply**.
8. In the **Success** dialog box, click **OK**.

   The newly-added physical interface appears in the **Physical interface** table.

Configure a Physical Interface

Use this task to configure a physical interface for your session delivery device.

1. Expand the **Configuration Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select a device and click **Load**.
3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.
4. In the navigation panel, click **Interfaces**.
5. In the **Interfaces** pane, select a physical interface in the **Physical interface** table and click **Edit**.
6. In the **Physical interface** pane, complete the following fields:

Name	Description
Auto-negotiation - 10/100Mbps field	If the default **enabled** is selected for the device, then this device and the device to which it is linked can automatically negotiate the duplex mode and speed for the link. If you want auto-negotiation disabled so that you can set these link parameters manually, select **disabled** to disable auto-negotiation and operate in **HALF** duplex mode (default) so that the devices do not engage in link negotiation or select **FULL** duplex mode to let both devices on a link send and receive packets simultaneously. You can set the connection speed to either **10** or **100** Mbps for **HALF** or **FULL** duplex mode.
Virtual MAC address field	Enter the virtual MAC address of the session delivery device.
Health score decrement for management interface failure% field	If you want to enter a value other than the default (**50** percent), enter the percentage that determines what is considered to be the active and standby health status of the physical interface for alarm purposes. This parameter is available if the **Maintenance** or **Control** parameter is selected for the **Operation type** field.

7. If you want to change the default alarm threshold for the physical interface (**minor**), click **Add** in the **Alarm threshold** section.

8. In the **Add Alarm threshold** dialog box, select from the following **Severity** drop-down list filter levels for syslog and SNMP alarms:
   - **minor**
   - **critical**
   - **major**
9. Click **Apply**.
10. In the **Success** dialog box, click **OK**.
11. Click **Apply** to finish configuring the physical interface.

Add a Network Interface

You must create a default network interface that is associated with your physical interface.

1. Expand the **Configuration Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select a device and click **Load**.
3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.
4. In the navigation panel, click **Interfaces**.
5. In the **Interfaces** pane, click **Add** in the **Network interface** table.

> **Note:**
>
> Click the arrow on the **Guidelines** box to view dependencies regarding your network interface.

6. In the **Add Network interface** dialog box, complete the following fields:

Name	Description
VLAN number field	If this network interface is not channelized, keep this port set to 0 (default). If this network interface is channelized, enter the appropriate VLAN number (sub-port ID).
Physical interface drop-down list	Click the physical interface to which this network interface corresponds in the drop down list.

7. Click **Apply**.
8. In the **Success** dialog box, click **OK**.

   The newly-added network interface appears in the **Network interface** table.

Configure a Network Interface

Use this task to configure your session delivery device to communicate with any network element.

1. Expand the **Configuration Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select a device and click **Load**.

3. In the navigation panel, click the **Global Settings** folder to expand the configuration navigation tree for the loaded device.
4. In the navigation panel, click **Interfaces**.
5. In the **Physical interface** table, click an existing physical interface.

   The network interface belonging to the selected physical interface appears in the **Network interface** table.
6. Select this network interface and click **Edit**.
7. The **Interfaces** pane displays. In the **Host** section complete the following fields to configure network interface parameters for the device:

Name	Description
Host name field	The host name of this network interface. This field is populated with **default**.
IP address drop-down list	The IP address of this network interface.
Subnet mask field	The subnet mask of this network interface.
Primary IP Address	The primary gateway that this network interface uses to communicate for the next hop route.
Secondary IP Address	The secondary gateway of this network interface (if applicable).

8. To configure parameters that monitor the health of the gateway, click **Add** in the **Gateway heartbeat** section.
9. In the **Add Gateway heartbeat** dialog box, complete the following fields:

Name	Description
State drop-down list	Select to **enable** or **disable** the gateway heartbeat feature. The default value is **enabled**.
Expected ARP message interval from gateway (sec) field	The number of seconds between heartbeats for the media interface gateway. Heartbeats are sent at this interval as long as the media interface is viable. The default value is **0**. The valid range is from **1** to **65535**. The value you configure in this field overrides any globally applicable value set in the gateway heartbeat interval parameter in the device HA node (redundancy) configuration.
Number of ARP request retransmissions (#) field	The number of heartbeat retries that you want sent to the media interface gateway before it is considered unreachable. The default value is **0**. The valid range is from **1** to **65535**.
ARP request timeout (sec) field	The heartbeat retry time-out value in seconds. The default value is **1**. The valid range is from **1** to **65535**. This parameter sets the amount of time between device ARP requests to establish media interface gateway communication after a media interface gateway failure.
Health score decrement-gateway or link failure field	The amount to subtract from the device health score if a media interface gateway heartbeat fails. If the value you set in the retry-time-out field is exceeded, this amount is subtracted from the overall health score of the system. The default value is **0**. The valid range is from **0** to **100**.

10. Click **Apply**.
11. To configure tunnel parameters for the device, click **Add** in the **Tunnel config** section.
12. In the **Add Tunnel config** dialog box, complete the following fields:

Name	Description
Name field	The unique name for the IPsec tunnel configuration.
Local IP address field	The local public IP address that terminates the IPSec tunnel.
Remote IP address field	The remote public IP address that terminates the IPSec tunnel.

13. Click **Apply**.
14. In the **DNS** section, complete the following fields to set a specific IP address for the network interface and others that are related to different types of management traffic:

Name	Description
Primary field	The domain name server (DNS) server for this network interface.
First backup field	The secondary DNS server for this network interface (if applicable).
Second backup field	The third DNS server for this network interface (if applicable).
Default domain name	The default domain for use with DNS queries.
DNS timeout	The DNS timeout value.

15. To configure (HIP) host-in-path firewall functions that are used to open well-known ports for services such as FTP, ICMP, SNMP, and Telnet over the media interfaces, complete the following fields:

Name	Description
HIP IP addresses box	The IPv4 addresses of the front panel network interfaces that are allowed to pass administrative traffic to the host. Adding HIP entries automatically opens the well-known port associated with a service.
FTP address field	The FTP interface IP address.
ICMP addresses box	The ICMP interface IP address(es).
SNMP address field	The SNMP interface IP address.
Telnet address field	The Telnet interface IP address.
SSH address field	The SSH interface IP address.

16. Click **Apply**.
17. In the **Success** dialog box, click **OK**.

Saving and Activating Session Delivery Configurations

> **Note:**
>
> During the save and activation process, other users cannot make changes to the session delivery device.

1. Expand the **Configuration Manager** slider and click **Devices**.
2. In the **Managed Devices** pane, select a device and click **Load**.
3. In the **Managed Devices** panel, click the **Home** folder to expand the configuration navigation tree for the loaded device.
4. Select the device and click **Update**.
5. In the **Update configuration** dialog box, click one of the following update operations:

- Save & activate configuration—(Default) Invokes the save/activate process
- Save configuration—Invokes the save process.
- Activate configuration—Makes this configuration the running configuration on the device.

6. Click **OK**.
7. In the **Information** dialog box, click **OK**.

   The operation you selected appears in the **Device tasks** table.
8. In the **Device tasks** table you can the operation row and click **View log** to get logging data for your device or save logging data to file on your local system.

4

View Summary Data for Devices

The following summary data is retrieved (through SNMP) for devices managed by the Oracle Communications Session Element Manager:

- The date and time of a login.
- The local date and time (with time zone adjustment) of the Oracle Communications Session Element Manager server.
- A list of all devices by either IP address or host name.
- The alarm (fault) status summary.
- Key performance indicators (KPI) for the top 20 alarm counts, health scores, top 20 CPU usage, top 20 memory usage, and top 20 call rate.
- A list of logged-in users with session start times and locations (IP addresses).

> **Note:**
>
> Top-level displays and the device-specific summaries are shown for the active Oracle Communications Session Element Manager device in the cluster. Statistics are not shown for an Oracle Communications Session Element Manager device in standby mode.

Refresh Summary View Data

Refresh Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. Click **Refresh** to update the table data.

Configure Auto Refresh

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. Click **Auto refresh** to configure a timed auto refresh interval for when the page contents update.
3. Click **OK**.

Stop Auto Refresh

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. Click **Stop Auto Refresh** to cancel a configured auto refresh interval for when the page contents update.

> **Note:**
>
> This button appears when the auto refresh function is configured only.

View Managed Devices Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Managed Devices** table, expand a device group folder(s) to navigate to the device you want to view.

Name	Description
Device	The managed device (or cluster) is underlined, which indicates you can select the device to view more summary data for this device. **Note:** You can hover your mouse and a pop-up displays with additional device (or device cluster) data. A round colored icon next to each device displays whether the device can be reached: • **Green**—The device (or both devices in a cluster) is reachable and information for this device can be retrieved through SNMP. • **Red**—The device cannot be contacted (or both devices in a cluster cannot be contacted). • **Yellow**—The standby device in the cluster is not reachable.
Target Name	The user-defined name for each device. An underscore (_) separates each target name for a cluster as in the example above, sd11_sd12.
Health Score	The system health percentage, with a system health percentage value of 100 (100%) being the healthiest.
Up Time	The system up time in hours, minutes, and seconds.
Software Version	The full release version of the device, which includes its software revision.
Hardware Version	The full identification of the device hardware platform.

View Key Performance Indicator Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.

2. In the **Device** column of the **Managed Devices** table, select the device you want to view. In the **Key Performance Indicators** table, the following information displays for your device:

Name	Description
Device	The device managed by Oracle Communications Session Element Manager and for which the data is retrieved through an SNMP query.
Location	The physical location for this managed device.
Up Time	The system up time for this device in days, hours, minutes, and seconds.
Health Score	The health score for this device. The health score range is 0 to 100. Health scores lower than 60 indicate the device is in poor health.
CPU	The percentage of CPU used in this device.
Memory	The percentage of memory used in this device.
Licensed Session Used	The number of concurrent calls from the system performance report and current signaling sessions.

3. Click **Refresh** to update KPI data.
4. Click **View Alarms** to view alarm data in Fault Manager.
5. Click **Back** to return to the main summary view display.

View Alarm Summary Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Device** column of the **Managed Devices** table, select the device you want to view. In the **Alarm Summary** table, a bar chart displays the alarm counts for all alarm categories for your device. You can mouse over a bar within the chart for the number of alarms that bar represents.

> **Note:**
>
> The system-default alarm colors for each alarm severity are:
>
> - **Critical**—Red
> - **Major**—Orange
> - **Minor**—Yellow
> - **All other alarms**—Green

See the *Change the Default Severity Alarm Colors* section in the *Security Manager* chapter for more information.

3. Click **Refresh** to update alarm summary data.
4. Click **View Alarms** to view alarm data in Fault Manager.
5. Click **Back** to return to the main summary view display.

View License Information

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Device** column of the **Managed Devices** table, select the device you want to view. In the **License Information** table, the following information displays for your device:

Name	Description
License Key	The license number for this device.
License Capacity	The maximum number of simultaneous sessions allowed by the device for all combined protocols.
Install Date	The device installation time and date in the following format: hh:mm:ss, month, day, year. Displays N/A if license is not enabled.
Start Date	The start time and date in the following format: hh:mm:ss, month, day, year. Displays N/A if the license is not enabled.
Expiration Date	The expiration time and date in the following format: hh:mm:ss, month, day, year and displays N/A if the license is not enabled.
Features	The features licensed for this device. Values are: • Interworking (IWF) • Quality of Service (QoS) • Acme Control Protocol (ACP) • Local Policy (LP) • Session Agent Group (SAG) • ACC (Allows the device to create connections and send CDRs to one or more RADIUS servers.) • High Availability (HA)
Protocols	The protocols licensed for this device. Values are: • SIP • MGCP • H.323

3. Click **Refresh** to update license data.
4. Click **View Alarms** to view alarm data in Fault Manager.
5. Click **Back** to return to the main summary view display.

View Health Score Data

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Health Scores** dialog box, you can mouse over a the pie chart to display health score percentage ranges for your devices or over individual devices in the **Device** list to display additional data for each device.

   The health score range is displayed with the following color scheme:

   - Green—Indicates a score range from 75 to 100, inclusive.
   - Orange—Indicates a score range from 50 to 74, inclusive.

- Red—Indicates a score below 50.

3. In the **Health Scores** dialog box, use the **Devices in Range** drop-down list to select the range of devices for which you want to view health scores:
   - **View All**
   - **75-100**—Average to good health.
   - **50-74**—Poor to average health.
   - **0-49**—Poor health.

View Top 20 Memory Usage

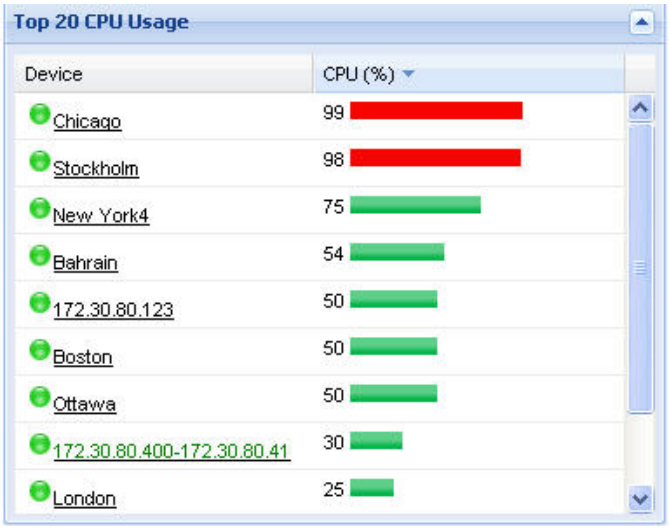
1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Top 20 Memory Usage** dialog box, a summary of the top 20 devices currently using the most memory the table is sorted by the descending percentage of memory. Mouse over each device to see additional information.

   The **Memory Usage** column displays the percentage of the memory utilization, followed by a colored bar, which corresponds with the memory usage percentage. The greater the percentage, the longer the bar. A red bar indicates a warning that memory usage is between 90% and 100% and a green bar indicates memory usage is below 90%.

View Top 20 CPU Usage

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Top 20 CPU Usage** dialog box, a summary of the top 20 devices with the most current percentage of CPU utilization is sorted by the descending percentage of CPU utilization. Mouse over each device to see additional information.

   The **CPU (%)** column displays the percentage of the CPU utilization, followed by a colored bar, which corresponds with the CPU usage percentage. The greater the percentage, the longer the bar. A red bar indicates a warning that CPU usage is between 90% and 100% and a green bar indicates memory usage is below 90%.

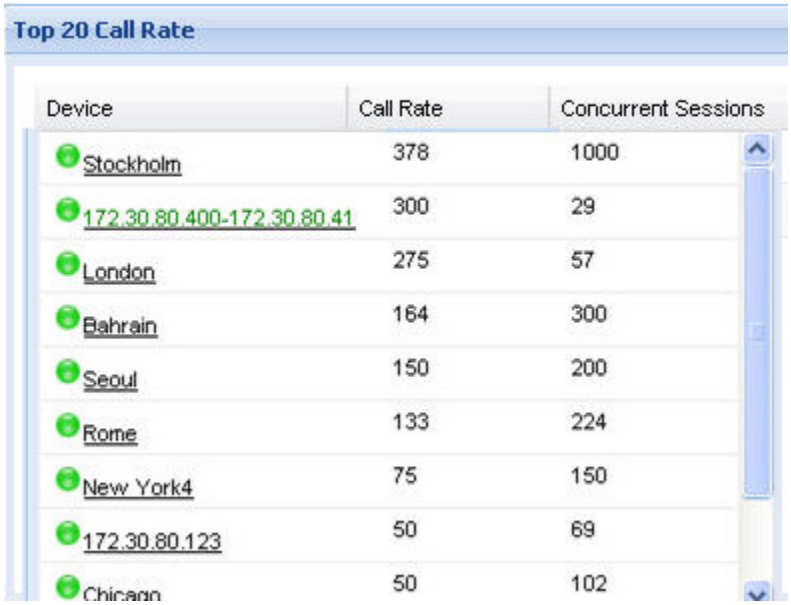


View Top 20 Alarm Counts

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Top 20 Alarm Counts** dialog box, a summary of the top 20 devices with generated alarms with critical and major designations. Mouse over each device to see additional information.

View Top 20 Call Rate

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. Expand the Dashboard Manager slider and click **Summary View**.
3. In the **Top 20 Call Rate** dialog box, a summary of the top 20 devices with highest number of active calls and concurrent sessions for each device. Mouse over each device to see additional information. For example:



View Logged In Users

1. Expand the **Dashboard Manager** slider and select **Summary view**.
2. In the **Logged In Users** dialog box, a summary of users logged into Oracle Communications Session Delivery Manager with the appropriate privileges is sorted in ascending alphanumeric order by default with the IP address of the user system.

> **Note:**
>
> The list does not display if you do not have administration-level privileges.

5
Fault Manager

Fault manager is used to view events, alarms and trap event settings. Events and alarm information is based on the Oracle® standard and proprietary Management Information Bases (MIBs). All SNMP traps generated from nodes are managed by Oracle Communications Session Element Manager. Both alarms and event trap notifications are generated when a bad (fault) event or alarm occurs on a node.

To receive notifications, ensure that SNMP communities and the MIB contact and trap receiver information is configured on your OSS/BSS system in order to receive fault notifications.

If you want more specific information about events, alarms, and MIBs that is not covered in this chapter, see the **Oracle Communications Core Session Manager MIB Reference Guide**.

Alarm and Event Configuration Tasks

The following sections describe the **Alarms** table and **Events** table, with their accompanying features. The **Events** table shows a one to one correspondence with all device traps and generated server events. The **Events** table maintains the precise history of all events created and recorded. The **Alarms** table summarizes the **Events** table by showing the most recent update for the specific categories, failed resources, and devices in each row. There may be several events generated in the **Alarms** table that correlate to events for a failed resource type for a device into one entry where the last known state and time is shown.

Manage How Alarms are Displayed

1. Expand the **Fault Manager** slider and select **Events**.
2. Glide your mouse over a column and click the drop-down list that appears next to any column heading.
3. Click the down arrow to display the menu.
4. Click **Sort Ascending** to sort the data in ascending order, or click **Sort Descending** to sort the data in descending order.
5. Click **Columns** sub-drop-down list to access a list of column names to edit.
6. Check a marked checkbox next to a column to hide it, or click an empty checkbox next to a column to display it.
7. In the alarms pane, select an alarm that you want to view and click **View**.

   > **Note:**
   >
   > Alternatively, you can double-click the alarm.

8. In the **Alarm detail** dialog box, view the following fields:

Name	Description
Annotation	The user-defined note pertaining to this alarm.
Acknowledged by	The user that acknowledged the alarm.
Time	The date and time this alarm was generated in hours, minutes, and seconds.
Modified time	The date and time the alarm was last modified.
Description	A short description of the alarm.
Source	The exact descriptive source of the alarm.
Source IP	The IP address from which this alarm was generated.
Failed resource	The resource responsible for this alarm.
Type	The type of trap associated with this alarm. For example, TrapRelayMonitor.
System up time	Length of time the system has been operational in hours, minutes, and seconds.
Severity	One of the following user-defined severity levels can display for a system alarm: **Note:** The number indicates the numerical severity level. • (0) EMERGENCY—The system is unusable. • (1) CRITICAL—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. The default color code is red. • (2) MAJOR—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but ceases to function. The default color code is salmon. • (3) MINOR—Error conditions exist. The functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. The default color code is orange. • (4) WARNING—Warning conditions exist. Some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly. The default color code is light yellow. • (5) NOTICE—Normal, but a significant condition exists. The default color is lime green. • (6) INFO—Informational messages are appearing. The default color code is yellow-green. • (7) TRACE—Trace messages appear. The default color is lime green. • (8) DEBUG—Debugging messages appear. The default color is lime green. • (9) DETAIL—Detailed messages appear. The default color is lime green.
Trap Name	The exact name of the trap associated with this alarm. For example, apNNCTrapRelayAliveNotification.
Trap Category	The category to which the alarm belongs. For example, NNC.

Name	Description
Source Group ID	(Hidden) The identity of the source group associated with this alarm.
Object ID	(Hidden) The object identifier (OID) associated with this alarm.

Manage How Events are Displayed

1. Expand the **Fault Manager** slider and select **Events**.
2. Glide your mouse over a column and click the drop-down list that appears next to any column heading.
3. Click the down arrow to display the menu.
4. Click **Sort Ascending** to sort the data in ascending order, or click **Sort Descending** to sort the data in descending order.
5. Click **Columns** sub-drop-down list to access a list of column names to edit.
6. Check a marked checkbox next to a column to hide it, or click an empty checkbox next to a column to display it.
7. In the events pane, select an event that you want to view and click **View**.

> **Note:**
>
> Alternatively, you can double-click the event.

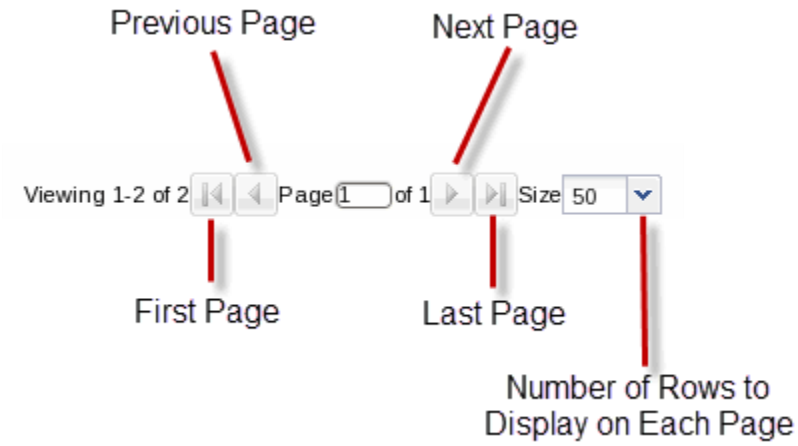
8. In the **Event detail** dialog box, view the following fields:

Name	Description
Time	The date and time this event was generated in hours, minutes, and seconds.
Description	A short description of the event.

Name	Description
Severity	One of the following user-defined severity levels can display for a system event: **Note:** The number indicates the numerical severity level. • (0) EMERGENCY—The system is unusable. • (1) CRITICAL—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. The default color code is red. • (2) MAJOR—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but ceases to function. The default color code is salmon. • (3) MINOR—Error conditions exist. The functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. The default color code is orange. • (4) WARNING—Warning conditions exist. Some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly. The default color code is light yellow. • (5) NOTICE—Normal, but a significant condition exists. The default color is lime green. • (6) INFO—Informational messages are appearing. The default color code is yellow-green. • (7) TRACE—Trace messages appear. The default color is lime green. • (8) DEBUG—Debugging messages appear. The default color is lime green. • (9) DETAIL—Detailed messages appear. The default color is lime green.
Default Severity	The system-defined severity level for this event.
Source	The exact descriptive source of the event.
Source IP	The IP address from which this event was generated.
Failed resource	The resource responsible for this event.
Type	The type of trap associated with this event. For example, TrapRelayMonitor.
Trap Name	The exact name of the trap associated with this event. For example, apNNCTrapRelayAliveNotification.
Trap Category	The category to which the event belongs. For example, NNC.
System up time	Length of time the system has been operational in hours, minutes, and seconds.
Source Group ID	(Hidden) The identity of the source group associated with this event.
Object ID	(Hidden) The object identifier (OID) associated with this event.

Navigate Multiple Fault Manager Pages

1. Expand the **Fault Manager** slider and choose from the following options:
   - **Events**
   - **Alarms**
2. At the top right area of the **Events** or **Alarms** pane, click the navigation icons to display the desired first page, previous page, next page, and the last page, etc.



Manage the Page View for Events and Alarms

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the alarms or events pane, you can select from the following actions:

Name	Description
Refresh button	Click to refresh the data in the table.
Show all button	Click to show all current alarms or events.

Search for Alarms or Events by Specifying a Criteria

You can search for events and alarms by specifying one, some, or all of the search selection criteria. For example, you can select alarms for a specific IP address during a specified date-time range.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the alarms or events pane, click **Search**.

3. In the **Filter search** dialog box, complete the following fields:

Name	Description
Date from field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The chosen date to filter event data begins at 12:00 AM (midnight) on the specified date.
Date to field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The date you select ends at 11:59:59 PM.
Source device field	The source name for this device.
Source IP field	The IP address for this source device.
Trap name drop-down list	Select the trap name.
Type drop-down list	Select the alarm type.
Severity drop-down list	Select the severity level for this alarm.

Change the Number of Alarms or Events in a Table

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. At the top of the events or alarms pane, click the **Size** drop-down list.

   Note:
   By default, 50 table items are displayed.
3. Click the appropriate value.

Save Alarms or Event Data to a File

You can save event or alarm data in the content area to a comma-separated values (CSV) file that stores table data (numbers and text) in plain-text form.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**

2. In the events or alarms pane, click **Save to file**.
3. In the save dialog box, select either to open the file or save the file.

> **Note:**
>
> If you save the file, the file is saved to your browser's default download location.

4. Click **OK**.

Delete Alarms or Events

The appropriate administrator privileges must be assigned to delete alarms or events.

> **Note:**
>
> Deleting an alarm in Oracle Communications Session Element Manager has no affect on the node because the node is unaware that Oracle Communications Session Element Manager displayed the alarm or deleted it from the alarms table.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the alarms or events table, click the alarm or event that you want to remove and click **Delete**.
3. In the **Delete** dialog box, click **Yes** to confirm the deletion of the alarm or event.

Specify a Criteria to Delete Alarms and Events

The appropriate administrator privileges must be assigned to delete alarms or events.

Use this task to specify one or more criterion for deleting alarms or events from Oracle Communications Session Element Manager.

1. Expand the **Fault Manager** slider and select from the following options:
   - **Events**
   - **Alarms**
2. In the events or alarms pane, click **Delete by criteria**.
3. In the **Delete event** dialog box, complete the following fields:

Name	Description
Please specify the delete choice field	Click to select either **Delete all** or **Delete by criteria**.

Name	Description
Date from field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The chosen date to filter event data begins at 12:00 AM (midnight) on the specified date.
Date to field	Click the calendar icon and select the month, year, and day and click **Today**. **Note:** The date you select ends at 11:59:59 PM.
Source device field	The source name for this device.
Source IP field	The IP address for this source device.
Trap name drop-down list	Select the trap name.
Type drop-down list	Select the alarm type.
Severity drop-down list	Select the severity level for this alarm or event.

4. Click **OK**.

Configure When Event and Alarm Data is Cleared

1. On the main menu, click **Settings** > **Faults** > **Fault configuration**.
2. In the **Fault configuration** dialog box, complete the following fields:

Name	Description
***Clear events older than (days)** field	The number of days events are retained in the database before the events are cleared. The default value is seven days. Zero indicates no event data is cleared
***Clear alarms older than (days)** field	The number of days alarms are retained in the database before the alarms are cleared. The default value is 14 days. Zero indicates no alarm data is cleared.
***Duplicate trap filter interval (minutes)** field	The number of minutes for when duplicate traps are cleared for events and alarms.

3. Click **OK**.
4. In the success dialog box, click **OK**.

Alarm Specific Configuration Tasks

Alarms play a significant role in determining the overall health of the system. An alarm is triggered when a condition or event happens within the hardware or software of a system (node). Alarms contain an alarm code, a severity level, a textual description of the event, and

the time the event occurred. The following sections describe how to configure the way alarms display in Oracle Communications Session Element Manager.

Configure the Auto Refresh Period for Alarm Data

1. Expand the **Fault Manager** slider and select **Alarms**.
2. Click **Auto refresh**.
3. In the **Auto refresh** dialog box, enter the number of seconds to refresh alarm data in the **Refresh Interval(secs)** field.
4. Click **OK**.

> **Note:**
>
> If you want to stop the auto-refresh function, click **Stop Auto Refresh**.

Add a Comment to an Alarm

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, click the alarm to which you want to add a comment and click **View**.
3. In the **Alarm detail** dialog box, click **Edit**.
4. Add your comments about this alarm in the **Description** field.
5. Click **OK**.

Enable Alarm Acknowledgement

The appropriate administrator privileges must be assigned to acknowledge alarms.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to acknowledge and click **Acknowledge**.
3. In the **Acknowledge** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.
5. Click the alarm to view an updated **Alarm detail** dialog box with the **Acknowledged by** and **Last modified** fields updated.
6. Click **OK**.

Disable Alarm Acknowledgement

The appropriate administrator privileges must be assigned to unacknowledge alarms.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to unacknowledge and click **Unacknowledge**. The Acknowledge dialog box appears.
3. In the **Unacknowledge** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.

Clear an Alarm

The appropriate administrator privileges must be assigned to clear alarms.

> **Note:**
>
> Clearing an alarm in Oracle Communications Session Element Manager has no affect on the node because the node is unaware that Oracle Communications Session Element Manager displayed the alarm or changed its severity to clear.

1. Expand the **Fault Manager** slider and select **Alarms**.
2. In the alarms table, select the alarm that you want to clear and click **Clear**.
3. In the **Clear** dialog box, click **Yes**.
4. In the **Info** dialog box, click **OK**.

Override Default Severity Levels for Alarm Trap Conditions

1. Expand the **Fault Manager** slider and select **Trap event setting**.
2. In the **SNMP Trap OID** dialog box, click the alarm trap you want to change from the **Trap Descriptor** scroll-down list.

   The information for the alarm trap appears in the **Severity Mapping** table below.
3. In the **Severity Mapping** table, click the **Current severity** column cell of the trap condition row that you want to modify.
4. In the drop-down list of severity levels, click the severity you want to apply. The new level appears in the Current Severity column.

   > **Note:**
   >
   > The **Default severity** column serves as a reference point and continues to show the default severity setting for the trap condition.
5. Click **Apply**.
6. In the Information dialog box, click **OK**.

Audible Alarms

The audible alarms system allows you to set off an audible sound when an activated alarm is triggered.

Alarm events are updated during each refresh cycle of the alarms table. Search functionality is disabled when audible alarms are active. The audible alarms cease to function upon exiting the Fault Manager navigation bar slider.

Audio Files

The Audible Alarms application comes with five alarm sounds (one for each severity). You may replace these files with your own as long as the new.wav files retain the same filenames. The files are located in the following directory:

<installed directory>\ACMEConsole\audibleAlarms

The filenames appear as:

- Audio_Emergency.wav
- Audio_Critical.wav
- Audio_Major.wav
- Audio_Minor.wav
- Audio_Warning.wav

Enable and Configure Audible Alarms

1. On the main menu, click **Settings** > **Alarms** > **Audible Alarms**
2. In the **Audible Alarms** dialog box, click the check box next to the severity categories that you want to enable an audible alarm. The categories are **Emergency**, **Critical**, **Major**, **Minor**, and **Warning**.
3. Click **OK**.
4. On the Oracle Communications Session Element Manager navigation bar, select **Fault Manager** > **Alarms**
5. Click **Start Audible Alarm**.

   The button toggles to **Stop Audible Alarm**.

6. If you want to shut down the audible alarms application, click **Stop Audible Alarm**.

   The button toggles to **Start Audible Alarm**.

Change the Default Severity Alarm Colors

1. On the main menu, click **Settings** > **Alarms** > **Alarm Colors**
2. In the **Alarm colors** dialog box, click the **Color** drop-down list next to the severity category and its default color.
3. In the pop-up color palette, click the new color that you want for the alarm.
4. Repeat the previous two steps if you want to configure more severity alarm colors.
5. Click **OK**.
6. In the success **Information** dialog box, click **OK**.

Event Types

Expand the **Fault Manager** slider and choose trap event setting to view the following event types.

Type	Description
apSysLog	Associates with the proprietary Oracle ap-slog.mib, which provides a method of gathering syslog messages generated by the system through SNMP.
apSysMgmt	Associates with the proprietary Oracle ap-smgmt.mib, which provides a means of gathering information about the status of the system.
ARP capacity	Measures the percentage of the ARP table in content addressable memory (CAM) utilization and is associated with the apSysMgmtGroup trap.
AuthTrap	Associates with the standard authenticationFailure trap. The SNMPv2 agent received a protocol message that was not properly authenticated.
ColdStart	Associates with the standard coldStart trap. The SNMPv2 agent is reinitializing itself and its configuration may have been altered.
CPU	Measures the percentage of CPU utilization and is associated with the apSysMgmtGroupTrap.
CPU load	Measures the percentage of CPU of application tasks has exceeded the threshold algd-load-limit
Discovery	This alarm displays the discovery status.
DoS	Displays the Oracle Denial of Service (DoS) protection proprietary trap.
Gateway	This alarm displays the status of gateway reachability and is associated with the apSysMgmtGatewayUnreachableTrap trap.
EMS-HA	This alarm is generated by the Oracle Communications Session Element Manager in a Oracle Communications Session Element Manager failover situation.
Enhanced DoS	Indicates a device exceeded configured thresholds and was denied access.
Fan	Indicates that the fan unit speed fell below the monitoring level.
H323 Stack	Describes the status of H.323 stack and is associated with the apSysMgmtH323InitFail trap.
HDR	This alarm indicates that the specified server becomes unreachable by the system collector.
Health	Indicates the system health percentages and is associated with the apSysMgmtGroupTrap trap.
I2C	Indicates that the Inter-IC bus (I2C) state changed from normal (1) to not functioning (7).
License	Associates with the proprietary Oracle ap-license.mib, which provides information about the status of your system licenses.
Link	This alarm is associated with the standard linkDown and linkUp traps: • linkDown—The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the up state to the down state. The ifOperStatus value indicates the other state. • linkUp—The SNMPv2 agent detects that the ifOperStatus object of an interface has transferred from the down state to the up state. The ifOperStatus value indicates the other state.
Media bandwidth	This alarm indicates that bandwidth allocation failed at a percentage higher or equal to the system's default threshold rate.
Media ports	This alarm indicates that port allocation failed at a percentage higher or equal to the system's default threshold rate.
Media realm	This alarm shows the status of the media realm and is associated with the apSysMgmtMediaUnknownRealm trap.
Memory	Displays the percentage of memory utilization and is associated with the apSysMgmtGroup trap.
Monitor	This alarm is associated with the proprietary Oracle ap-env-monitor.mib, which gathers information about fan speed, voltage, temperature, and power supply for the system. It also sends out traps when status changes occur.

Type	Description
NAT capacity	Shows the percentage of NAT table (in CAM) utilization.
NTP Clock Skew	This alarm indicates NTP had to adjust the clock by more than 1000 seconds.
NTP server	This alarm indicates that the specified NTP server is unreachable.
NTP service	This alarm indicates that all configured NTP servers are unreachable.
Polling	Describes reachability information for connected devices.
Power	This alarm indicates the status of power supply and is associated with the apEnvMonStatusChangeNotification trap.
Realm Minutes Exceeded	This alarm describes the monthly minutes exceeded for a realm.
RADIUS Servers	This alarm shows the status of the RADIUS server.
Reboot	This alarm shows the proprietary version of the standard coldStart trap.
Redundancy	This alarm indicates that a state change occurred on either the primary or secondary system in a redundant (HA) pair.
Save-config	Indicates that an error occurred while the system was trying to save the configuration to memory.
Session agent	This alarm displays the session agent information, which includes the hostname, IP address, status, and the reason for the status. This alarm is associated with the apSysMgmtStatusChange trap.
Single unit redundancy	This alarm shows if the status of a slot changed. The varbinds contain the new information for the slot.
Surrogate registration	This alarm shows the status of surrogate registration and associated with the apSysMgmtSurrogateRegFailed trap.
Task	This alarm indicates that there is a suspended task and is associated with the apSysMgmtTaskSuspendTrap trap.
Temperature change	Indicates the system temperature and is associated with the apSysMgmtTempTrap trap.

Enabling Alarm Synchronization

You must have administrator privileges to do this task.

Use the following steps to synchronize the displayed alarms in Oracle Communications Session Element Manager with those maintained on session delivery devices that support alarm synchronization.

1. On the Oracle Communications Session Element Manager navigation bar, choose **Device Manager** > **Devices**.
2. In the **Managed Devices - Group View** table tree, expand the tree and click the device for which you want to enable alarm synchronization.
3. Click **Admin** > **Synchronize alarms**.
4. In the **Synchronize alarms** dialog box, click **Yes**.
5. In the success dialog box, click **OK**.

Fault Email Notifications

Oracle Communications Session Element Manager can trigger automatic email notifications when reporting alarms for certain severities. You can configure the appropriate email addresses that match each alarm severity.

Configure Email Notifications for Fault Occurrences

With appropriate administrator privileges assigned, you can assign fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.
2. In the **Fault email recipients** dialog box, click **Add**.
3. In the **Add email** dialog box, complete the following fields:

Name	Description
***Email address** field	The recipient email address attached to the alarm severity.
Severity drop-down list	Select the severity level for this email notification. The levels are **Emergency**, **Critical**, **Major**, **Minor**, **Notice**, **Warning**, **Info**, **Trace**, **Debug**, and **Unknown**.
Notify on clear check box	Check the check box to send a fault notification on all clear events. This option is only available for the following severity levels: **Emergency**, **Critical**, **Major**, and **Minor**.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. In the **Fault email recipients** dialog box, the configured email address appears in the table. Click **OK**.

Delete Fault Email Notifications

With appropriate administrator privileges assigned, you can delete fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.
2. In the **Fault email recipients** dialog box, select the email address you want to remove and click **Delete**.
3. In the **Delete** dialog box, click **Yes**.
4. In the success dialog box, click **OK**.
5. In the **Fault email recipients** dialog box, the email address no longer appears in the table. Click **OK**

Edit Fault Email Notifications

With appropriate administrator privileges assigned, you can edit fault email notifications.

1. On the main menu, click **Settings** > **Faults** > **Fault email notifications**.
2. In the **Fault email recipients** dialog box, select the email address you want to edit and click **Edit**.
3. In the **Edit email** dialog box, edit the following fields:

Name	Description
***Email address** field	The recipient email address attached to the alarm severity.

Name	Description
Severity drop-down list	Select the severity level for this email notification. The levels are **Emergency**, **Critical**, **Major**, **Minor**, **Notice**, **Warning**, **Info**, **Trace**, **Debug**, and **Unknown**.
Notify on clear check box	Check the check box to send a fault notification on all clear events. This option is only available for the following severity levels: **Emergency**, **Critical**, **Major**, and **Minor**.

4. Click **OK**.
5. In the success dialog box, click **OK**.
6. In the **Fault email recipients** dialog box, the edited email address appears in the table. Click **OK**

Configure External Trap Receivers

This section describes the Oracle Communications Session Element Manager traps contained in the Oracle Communications Session Element Manager MIB and the configuration of external trap receivers. You must configure an external server to be the receiver of these traps.

Oracle Communications Session Element Manager generates traps when it detects the following:

- Failure to save a device configuration
- Failure to activate a device configuration
- Node status change from reachable to unreachable

Oracle Communications Session Element Manager Traps

Oracle Communications Session Element Manager generates the following notification traps:

Trap	Description
apEMSSaveFailure	This trap is generated when Oracle Communications Session Element Manager fails to save a configuration. The trap is generated by a save failure whether initiated by the SOAP XML API or Oracle Communications Session Element Manager GUI for the save/activate, save, or offline save operations. The trap contains the node ID of the device, the start and stop time of the save configuration attempt, and the user initiating the save operation.
apEMSActivateFailure	This trap is generated when Oracle Communications Session Element Manager fails to activate a configuration, whether initiated from the SOAP XML API or the Oracle Communications Session Element Manager GUI for the save/activate or activate operations.
apEMSNodeUnreachable	This trap is generated when the status of a node changes from reachable to unreachable. The trap contains the node ID of the device and the time of the event.
apEMSNodeUnreachableClear	Clearing condition trap. Generated when the status of a node changes from unreachable to reachable. The trap contains the node ID of the device and the time of the event.

Notification Objects

The Oracle Oracle Communications Session Element Manager MIB also lists the following notification objects contained in the generated traps.

Notification Objects	Description
apEMSNodeID	The identifier for a Oracle Communications Session Element Manager node that appears on the navigation tree in the Active configuration area on the Discovery table in the Host Name/IP Address column.
apCentralStartTime	The time configured on the Oracle Communications Session Element Manager server when an event occurs.
apEMSDateTime	The time configured on the Oracle Communications Session Element Manager server when an event completes.
apEMSUser	The user initiating the function. If the function was automatically initiated by the Oracle Communications Session Element Manager application, the user is system.
apEMDeviceAddres s	The address for a device being managed.

Add External Trap Receivers

An external trap receiver is a device that you use as the SNMP trap destination, instead of the device where Oracle Communications Session Element Manager is installed. When you configure the external trap receiver, you enter its address and port. The combination of IP address and port must be unique for each configured trap receiver.

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, click **Add**.
3. In the **Add trap receiver** dialog box, complete the following fields:

Name	Description
***IP address** field	The IP address of the server receiving traps.
***UDP port** field	The port number for the server receiving the traps or retain the default value of **162**.
***Community string** field	The name of the SNMP community to which the server receiving traps belongs or retain the default value **public**.
SNMP version drop-down list	The version of SNMP. SNMP Version 2 (**V2**) is chosen by default.
Forward enabled check box	Check the check box if you want to allow the trap to be forwarded to a client.

Name	Description
Severity level drop-down list	Select from the following trap severity levels: • **Indeterminate**—The trap severity cannot be determined because of the nature of the information contained in the trap. • **Critical**—The alert indicates that action must be taken immediately. If no actions are taken, there may be physical, permanent, and irreparable damage to your system. • **Major**—Critical conditions exist. The functionality has been seriously compromised and a loss of functionality, hanging applications, and dropped packets may occur. If no actions are taken, your system suffers no physical harm, but it ceases to function. • **Minor**—Error conditions exist. Functionality has been impaired to a certain degree and you might experience compromised functionality. There is no physical harm to your system, but you need to take actions to keep your system operating properly. • **Warning**—Warning conditions exist. There are some irregularities in performance. These conditions are noteworthy and you should take actions to keep your system operating properly.
Format field	Select from the following trap formats: • **OC SDM** radio button—**Oracle Communications Session Delivery Manager** format. – **OC SDM traps** check box is pre-selected for **Oracle Communications Session Delivery Manager** traps. • **ITU X.733** radio button—International Telecommunication Union Alarm Model format defined in recommendation X.733. – **OC SDM traps** check box is pre-selected for **Oracle Communications Session Delivery Manager** by default. You can un-check this check box. – **SBC traps** check box—Oracle Communications Session Border Controller traps. **Note:** If this check box is checked, you can specify that traps for the device can be forwarded to the destination. If the **Select devices** radio button is chosen, you can select a device from the **Managed devices** box and click the **Add** arrow button to add the trap device to the **Selected trap source devices** box. You can remove a trap device by selecting it and clicking the **Remove** arrow button.

4. Click **OK**.

   The new trap is added to the table in the **Trap receivers configuration** dialog box.

Synchronize an External Trap Receiver to Validate the Health of a Device

Use this task to configure alarms or events on the Oracle Communications Session Element Manager to be resent (forwarded) out of the northbound interface to the connected destination

trap receiver (device) in order to synchronize the alarms or events so that the health of the connected device can be determined.

> **Note:**
>
> You must add an external trap receiver device before doing this task.

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, select the trap receiver that you want to edit and click **Sync**.
3. In the **Trap receiver alarm synchronization** dialog box, complete the following fields:

Name	Description
Synchronization from radio button	Click the **Event** radio button or **Alarm** radio button to resend events or alarms to the connected destination trap receiver.
Minimum severity level drop-down list	Select from the following security levels to send all existing events or alarms with this severity level or higher to its destination trap receiver: • **Indeterminate**—Clear all events and synchronize from when they were cleared. • **Critical**—Send critical events or alarms. • **Major**—Send major and critical events or alarms. • **Minor**—Send minor, major, and critical events or alarms. • **Warning**—Send warning, minor, major, and critical events or alarms. • **Clear**—Clear all alarms and synchronize from when they were cleared.
Date and time from: fields	Click the calendar icon to select the synchronization start date and time.
Date and time to: fields	Click the calendar icon to select the synchronization end date and time.

4. Click **OK**.

Add the Heartbeat Trap to Monitor Server Availability

The heartbeat trap (apOCSDMServerHeartbeatReachable) can be manually started and stopped to periodically monitor the availability of the Oracle Communications Session Element Manager from the northbound interface. This heartbeat trap is sent (forwarded) out of the northbound interface as an event (INFO) to the connected destination trap receiver of a management device. A problem can be detected by the management device if no heartbeat trap is received by its trap receiver during the specified interval due to either the failure of a single

server or server cluster, or if SNMP administrative changes affected the connectivity between the server and management device.

> **Note:**
>
> You must add an external trap receiver device to Oracle Communications Session Element Manager before doing this task.

The heartbeat trap is disabled by default. Use the following steps to specify the heartbeat trap send interval, and initiate the sending or termination of a heartbeat trap.

1. On the main menu, click **Settings** > **Faults** > **Heartbeat Traps**.
2. In the **Configure heartbeat SNMP trap interval** dialog box, complete the following fields:

Name	Description
Interval (minutes) drop-down list	Select the number of minutes to send the heartbeat trap. The range increments in 5 (default), 10, 15, 30 and 60 minutes.
Start field	(Read-only) The time the last heartbeat trap was started.
Stop field	(Read-only) The time the last heartbeat trap was stopped.
Trap time stamp field	(Read-only) The time stamp for when the last heartbeat trap was sent.

3. Click **Apply** to update the interval change.
4. Click **Start** to send the heartbeat trap. The heartbeat trap is sent at the interval that you specify.
5. Click **Stop** to terminate the heartbeat trap.
6. Click **Refresh** to see the most current trap time stamp information for exactly when the last heartbeat trap was sent.

Edit External Trap Receivers

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, select the trap that you want to edit and click **Edit**.
3. In the **Edit trap receiver** dialog box, edit the fields described in the **Add External Trap Receivers** section and click **OK**.

Delete External Trap Receivers

1. On the main menu, click **Settings** > **Faults** > **Trap receivers**.
2. In the **Trap receivers configuration** dialog box, choose the trap that you want to delete and click **Delete**.
3. In the confirmation dialog box, click **Yes**.
4. In the success dialog box click **OK**.

   The trap is removed from the table in the **Trap receivers configuration** dialog box.

6
Performance Manager

The **Performance Manager** slider has a navigation pane that contains a set of performance groups (that appear when a device is selected) that can be accessed to get different kinds of statistical and state information for your managed Oracle Communications Session Element Manager device(s).

Performance Manager collects and analyses data received or sent over product devices over time by its software (through SNMP MIBs). This statistical and state data is displayed on-demand when you access a performance group. Information for this performance group is displayed in the **Performance Manager** pane. Use this chapter to find information for each performance group.

> **Note:**
>
> The SNMP community parameter must be configured for product devices from which performance data is being viewed. See the *Configuration Manager* chapter for more information.

View Performance Groups for a Device

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, select and expand a device group folder. The **Devices** pane displays the following columns for each device:

Name	Description
Device	The IP address for the device.
Target Name	The descriptive name of the device.
Software Version	The software version running on the device.
Hardware Version	The hardware version of the device.

> **Note:**
>
> The default device group folder is **Home**.

3. Select a device in the device group folder, and click **View**.

   The **Performance Groups** folder appears with its performance groups in the navigation pane below the expanded **Performance Manager** slider.

> **Note:**
>
> If you click a performance group and do not select a device, statistics for the last device are loaded when you click **View**.

4. Select the performance group you want.

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the individual performance groups described in this chapter. See your device product documentation for more information. When you access a performance group data for devices that belong to a cluster, data for both devices appears in the content area. The title of each panel is the device name (or IP address) of each device in the cluster.

Save Performance Group Data

You can save performance group data that belongs to a device to a text file in comma separated values (CSV) format.

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Save to file**.
6. In the browser dialog box used to save the file, select the save the file option (for example, in Firefox, select **Save File**).

   > **Note:**
   >
   > The saved file is saved in the following format:

   ```
   <stats screen name>-<tab name>-<date> <hh-mm-ss>.csv
   ```

   For example:

   ```
   System-General-2011-06-10 13-53-21.csv
   ```
7. Click **OK** to save the file to your local directory and close the window.

Refresh Performance Group Data

Use the following sections to refresh the statistics displayed for a performance group that belongs to a device.

Refresh a Performance Group

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Refresh**.

Configure the Automatic Refresh Interval for a Performance Group

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Auto refresh**.
6. In the **Auto Refresh** dialog box, enter the number of seconds you want to configure for the auto refresh of performance data from this device performance group.
7. Click **OK**.

Stop the Automatic Refresh of a Performance Group

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Under the **Performance Groups** folder, select the performance group you want.
5. In the performance group pane, click **Stop auto refresh**.

   The automatic refresh function of performance data stops.

View Performance Group Data

The following sections describe the types performance group data that can be viewed for a Oracle Communications Session Element Manager device.

System

View General Data for a System

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. In the **Performance Groups** folder, select **System**.
5. In the System pane, select the **General** tab. The following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
CPU utilization (%)	The total percentage of CPU utilization measured in one second.
CPU Application load rate	The average load rate of the service applications taken over a period of up to 10 seconds.
Memory utilization (%)	The percentage of memory utilization.
CAM utilization (%) - media	The percentage of network address translation (NAT) table (in content addressable memory (CAM)) utilization.
CAM utilization (%) - ARP	The percentage of address resolution protocol (ARP) table (in CAM) utilization.
License capacity	The percentage of licensed sessions currently in progress.
Health score (%)	The system health percentage (a value of 100 (percent) is the healthiest).
Redundancy state	For clusters, the information about the state of each device in the cluster. Values are: • **active** • **standby**
Current signaling sessions (SIP, H.323, and MGCP)	The total number of global concurrent sessions at the moment.
Current signaling rate (SIP, H.323, and MGCP) (CPS)	The number of global calls per second.

Name	Description
I2C bus state	State of the environmental monitor located in the chassis. The values are: • **online**—Denotes regular call processing. • **offline**—Denotes no call processing but other administrative functions are available.

View Identification Data for a System

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. In the **Performance Groups** folder, select **System**.
5. In the System pane, select the **Identification** tab. The following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
System name	Administratively-assigned name for this node. By convention, this is the node's fully-qualified domain name. If the name is unknown, the value is the zero-length string
System contact	Textual identification of the contact person for this node, together with information on how to contact this person. If no contact information is known, the value is the zero-length string
System location	Physical location of this node. If the location is unknown, the field is left blank
System description	Textual description of the entity. This value includes the full name and version identification of the system's hardware type, software operating-system, and networking software
System objectID	Vendor's authoritative identification of the network management subsystem contained in the entity. This value is allocated within the SMI enterprises subtree (1.3.6.1.4.1) and provides an easy and unambiguous means for determining what kind of box is being managed
System uptime	Time (in hundredths of a second) since the network management portion of the system was last re-initialized

SNMP

View SNMP Performance Group Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **SNMP** performance group.
5. In the SNMP performance group pane, the following general SNMP data is displayed:

Name	Description
Authentication traps	The SNMP entity is permitted to generate authenticationFailure traps.
In packets	The total number of messages delivered to the SNMP entity from the transport service.
Out packets	The total number of SNMP messages passed from the SNMP protocol entity to the transport service.

The following **SNMP inbound details** data is displayed:

Name	Description
Bad versions	The total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version.
Bad community names	The total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity.
Bad community uses	The total number of SNMP messages delivered to the SNMP entity which represented an SNMP operation which was not allowed by the SNMP community named in the message.
ASN parse errors	The total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages.
Silent drops	The total number of GetRequest-PDUs, GetNextRequest-PDUs, GetBulkRequest-PDUs, SetRequest-PDUs, and InformRequest-PDUs delivered to the SNMP entity that were silently dropped. They were dropped because the size of a reply containing an alternate Response-PDU with an empty variable-bindings field was greater than either a local constraint or the maximum message size associated with the originator of the request.
Too bigs	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig.

Name	Description
No such names	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is noSuchName.
Bad values	The total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is badValue.
Read only	The total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is readOnly. **Note:** Generating an SNMP PDU that contains the value readOnly in the error-status field is a protocol error. This value is provided to detect incorrect implementations of SNMP.
General errors	The total number of valid SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is genErr.
Total requested variables	The total number of MIB objects retrieved successfully by the SNMP protocol entity as the result of receiving valid SNMP Get-Request and Get-Next PDUs.
Total set variables	The total number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP set-Request PDUs.
Get requests	The total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity.
Get next requests	The total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity.
Set requests	The total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity.
Get responses	The total number of SNMP Get-Responses that have been accepted and processed by the SNMP protocol entity.
Traps	The total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity.

The following **SNMP outbound details** data is displayed:

Name	Description
Too bigs	The total number of SNMP PDUs generated by the SNMP protocol entity and for which the value of the error-status field is tooBig.
No such names	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is noSuchName.
Bad values	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is badValue.
General errors	The total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is genErr.
Get responses	The total number of SNMP Get-Responses generated by the SNMP protocol entity.
Traps	The total number of SNMP Trap PDUs generated by the SNMP protocol entity.

IP

View General IP Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **General** tab.
6. In the **General** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Total datagrams received	The total number of input datagrams received from interfaces, including those received in error.

Name	Description
Forwarding capability	This indicates whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by, but not addressed to, this entity. IP gateways forward datagrams. IP hosts do not (except those source-routed via the host). Note that for some nodes, this object may take on only a subset of the values possible. Accordingly, it is appropriate for an agent to return a badValue response if a management station attempts to change this object to an inappropriate value.
Default time-to-live	The default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol.
Reassembly timeout(s)	The maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.
Reassemblies required	The number of IP fragments received which needed to be reassembled at this entity.
Reassembled datagrams	The number of IP datagrams successfully re-assembled.
Fragmented datagrams	The number of IP datagrams that have been successfully fragmented at this entity.
Fragmentation failures	The number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be (for example, because their Don't Fragment flag was set).
Created due to fragmentation	The number of IP datagram fragments that have been generated as a result of fragmentation at this entity.
Routing discards	The number of routing entries that were discarded although they were valid. A reason for discard could be to free up buffer space for other routing entries.

Inbound Details

Name	Description
Delivered	The total number of input datagrams successfully delivered to IP user-protocols including Internet Control Message Protocol (ICMP).
Header errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on.

Name	Description
Address errors	The number of input datagrams discarded because the IP address in their IP header's destination field was not a valid address to be received at this entity. This count includes invalid addresses (for example., 0.0.0.0) and addresses of unsupported Classes (for example., Class E). For entities which are not IP Gateways and therefore do not forward datagrams, this counter includes datagrams discarded because the destination address was not a local address.
Unknown protocols	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Discards	The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space). **Note:** This counter does not include any datagrams discarded while awaiting re-assembly.

Outbound details

Name	Description
Requests	The total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. **Note:** This counter does not include any datagrams counted in ipForwDatagrams.

Name	Description
Discards	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space). **Note:** This counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.
No routes	Number of IP datagrams discarded because a route could not be found to transmit them to their destination. **Note:** This counter includes any packets counted in ipForwDatagrams which meet this no-route criterion. This includes any datagrams which a host cannot route because all of its default gateways are down.

View Address Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **Addresses** tab.
6. In the **Addresses** tab, the following information displays for device control and maintenance interfaces (wancom and loopback):

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
IP Address	The IP address to which this entry's addressing information pertains.
Interface Index	The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of ifIndex.
Network mask	Subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the host bits set to 0.
Broadcast address	The value of the least-significant bit in the IP broadcast address used for sending datagrams on the (logical) interface associated with the IP address of this entry. For example, when the Internet standard all-ones broadcast address is used, the value is 1. This value applies to both the subnet and network broadcasts addresses used by the entity on this (logical) interface.
Max reassembly size	The size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface.

View Interface Statistics

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **Interface stats** tab.
6. In the **Interface stats** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	The unique value for each interface. Value has a range between 1 and the value of ifNumber and must remain constant at least from one re-initialization of the entity's NMS to the next re-initialization.
Name	The interface name.

Name	Description
Description	The text string containing information about the interface. This string includes the name of the manufacturer, the product name, and the version of the hardware interface.
Type	The information about the type of interface, distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack.
MTU	The size of the largest datagram which can be sent/received on the interface, specified in octets. For interfaces that transmit network datagrams, this is the size of the largest network datagram that can be sent on the interface
Speed	The estimate of the current bandwidth of the interface in bits per second. For interfaces which do not vary in bandwidth or for those where an accurate estimation cannot be made, it contains the nominal bandwidth.
Physical address	The address of the interface at the protocol layer immediately below the network layer in the protocol stack. For interfaces which do not have such an address (for example, a serial line), it contains an octet string of zero length.
Admin status	Current administrative state of the interface. The values are: • **up** • **down** • **testing**
Operational status	Current operational state of the interface. The values are: • **up** • **down** • **testing**
Last change time	The value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then it contains a zero value.
In octets	The total number of octets received on the interface, including framing characters.
Unicast packets in	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Non-unicast packets in	The number of non-unicast (for example, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol.
In discards	The number of inbound packets which were chosen to be discarded although no errors had been detected to prevent their being delivered to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
In errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Name	Description
In unknown protocols	For packet-oriented interfaces, the number of packets received through the interface which were discarded because of an unknown or unsupported protocol. For character-oriented or fixed-length interfaces that support protocol multiplexing, the number of transmission units received via the interface which were discarded because of an unknown or unsupported protocol. For any interface that does not support protocol multiplexing, this counter is always zero.
Out octets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Unicast packets out	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Non-unicast packets out	The total number of packets that higher-level protocols requested be transmitted to a non-unicast (that is, a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent.
Out discards	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Out errors	The number of outbound packets that could not be transmitted because of errors.

View Interface Statistics Utilization Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **Interface stats utilization** tab.
6. In the **Interface stats utilization** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Name	The text string containing the name of the media interface. The name is the one assigned by the local device that can be a text name or a port number, depending on the interface naming syntax of the device.
Rx Utilization	The receive media ports that are used for media ports indexed by IF index.
Tx Utilization	The transmit media ports that are used for media ports indexed by IF index.

View Extended Interface Statistics Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **Extended interface stats** tab.
6. In the **Extended interface stats** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Name	The text string containing the name of the interface. The name is the one assigned by the local device. It could be a text name or a port number, depending on the interface naming syntax of the device.

In

Name	Description
Multicast packets	The number of packets delivered from this layer to a higher layer that were addressed to a multicast address. For a MAC layer protocol, it includes both group and functional addresses.
Broadcast packets	The number of packets delivered by this layer to a higher level that were addressed to a broadcast address.

Out

Name	Description
Multicast packets	The number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent.
Broadcast packets	The number of packets higher-level protocols requested to be transmitted that were addressed to a broadcast address at this layer, including those discarded or not sent.

HC in

Name	Description
Octets	The total number of octets received on the interface, including framing characters.
Unicast packets	The number of packets delivered by this layer to a higher layer that were not addressed to a multicast or broadcast address at this layer.
Multicast packets	The number of packets delivered by this layer to a higher layer that were addressed to a multicast address at this layer. For a MAC layer protocol, this includes both group and functional addresses.
Broadcast packets	The number of packets delivered by this layer to a higher layer that were addressed to a broadcast address at this layer.

HC out

Name	Description
Octets	Total number of octets transmitted out of the interface, including framing characters.
Unicast packets	Total number of packets that higher-level protocols requested be transmitted that were not addressed to a multicast or broadcast address at this layer; including those discarded or not sent.
Multicast packets	The total number of packets that higher-level protocols requested be transmitted that were addressed to a multicast address at this layer, including those discarded or not sent. For a MAC layer protocol, this includes both the group and functional addresses.
Broadcast packets	The total number of packets that higher-level protocols requested be transmitted that were addressed to a broadcast address at this layer; including those discarded or not sent.
Link up/down trap enable	This field indicates whether linkUp/linkDown traps should be generated for this interface. The value should be enabled(1) for interfaces that do no operate on top of any other interface and disabled(2) otherwise.

Name	Description
High Speed	The estimate of the interface's current bandwidth in units of 1,000,000 bits per second. If a value of n is reported, the speed of the interface is in the range of n-500,00 to n+499,999. For interfaces that do no vary in bandwidth or for those where no accurate estimation can be made, a nominal bandwidth is given.
Connector Present	If the interface layer has a physical connector, the value is true(1). Otherwise it is false(2).

View ICMP Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **ICMP** tab.
6. In the **ICMP** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Inbound statistics

Name	Description
Messages	The total number of ICMP messages which the device received. **Note:** This counter includes all those counted by icmpInErrors.
Errors	The number of ICMP messages which the device received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).
Destination unreachables	The number of ICMP Destination Unreachable messages received.
Time exceeded	The number of ICMP Time Exceeded messages received.

Name	Description
Parameter problems	The number of ICMP Parameter Problem messages received.
Source quenches	The number of ICMP Source Quench messages received.
Redirects	The number of ICMP Redirect messages received.
Echoes	The number of ICMP Echo (request) messages received.
Echo replies	The number of ICMP Echo Reply messages received.
Timestamps	The number of ICMP Timestamp (request) messages received.
Timestamp replies	The number of ICMP Timestamp Reply messages received.
Address masks	The number of ICMP Address Mask Request messages received.
Address mask replies	The number of ICMP Address Mask Reply messages received.

Outbound statistics

Name	Description
Messages	The total number of ICMP messages which the Oracle Communications Session Delivery product attempted to send. This counter includes all those counted by icmpOutErrors.
Errors	The number of ICMP messages which the Oracle Communications Session Delivery product did not send due to problems discovered within ICMP such as a lack of buffers. This value does not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.
Destination unreachables	The number of ICMP Destination Unreachable messages sent.
Time exceeded	The number of ICMP Time Exceeded messages sent.
Parameter problems	The number of ICMP Parameter Problem messages sent.
Source quenches	The number of ICMP Source Quench messages sent.
Redirects	The number of ICMP Redirect messages sent.
Echoes	The number of ICMP Echo (request) messages sent.
Echo replies	The number of ICMP Echo Reply messages sent.
Timestamps	The number of ICMP Timestamp (request) messages sent.
Timestamp replies	The number of ICMP Timestamp Reply messages sent.

Name	Description
Address masks	The number of ICMP Address Mask Request messages sent.
Address mask replies	The number of ICMP Address Mask Reply messages sent.

Global TCP

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **Global TCP** tab.
6. In the **Global TCP** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Retransmission algorithm	The algorithm used to determine the timeout value used for retransmitting unacknowledged octets.
Retransmission timeout min (ms)	The minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre, an object of this type has the semantics of the LBOUND quantity described in RFC 793.
Retransmission timeout max (ms)	The maximum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects of this type depend upon the algorithm used to determine the retransmission timeout. In particular, when the timeout algorithm is rsre, an object of this type has the semantics of the UBOUND quantity described in RFC 793.
Max connections	The total number of TCP connections the Oracle Communications Session Delivery product supports. In entities where the maximum number of connections is dynamic, this object contains the value -1.

Name	Description
Active opens	The number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state.
Passive opens	The number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state.
Attempt fails	The number of times TCP connections made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections made a direct transition to the LISTEN state from the SYN-RCVD state.
Established resets	The number of times TCP connections made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.
Current established	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
In segments	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Out segments	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.
Retransmitted segments	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
In errors	The total number of segments received in error (for example, bad TCP checksums). Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.
Out resets	The number of TCP segments sent containing the RST flag. Discontinuities in the value of this counter are indicated via discontinuities in the value of sysUpTime.

View TCP Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **TCP** tab.
6. In the **TCP** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Local address	The local IP address for this TCP connection. In the case of a connection in the listen state, the value is 0.0.0.0
Local port	The local port number for this TCP connection.
Remote address	The remote IP address for this TCP connection.
Remote port	The remote port number for this TCP connection.
State	The state of this TCP connection. Valid values are: • **closed** • **listen** • **established**

View Global UDP Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **Global UDP** tab.
6. In the **Global UDP** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
In datagrams	The total number of UDP datagrams delivered to UDP users.
No Ports	The total number of received UDP datagrams for which there was no application at the destination port.

Name	Description
In errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
Out datagrams	The total number of UDP datagrams sent from this device.

UDP

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IP** performance group.
5. In the IP performance group pane, select the **UDP** tab.
6. In the **UDP** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Local address	The local IP address for this UDP listener. In the case of a UDP listener which is willing to accept datagrams for any IP interface associated with the node, the value is 0.0.0.0.
Local port	The local port number for this UDP listener.

> **Note:**
>
> The message **No data** indicates there is no performance data for this performance category for this device.

Environmental

View Voltage Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

The **Performance Groups** folder appears in the navigation pane with performance groups below it.

4. Select the **Environmental** performance group.
5. In the Environmental performance group pane, select the **Voltage** tab.
6. In the **Voltage** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Voltage type	Value which indicates the sensor monitoring voltage. Values are: • v2p5- 2.5v sensor. This monitors L3 cache core voltage, micro-processor and co-processor I/O voltage, and Field-Programmable Gate Array (FPGA) memories I/O voltage. • v3p3 - 3.3V sensor. This monitors general TTL supply rail, control logic, micro-processor; micro-processor and co-processor; and SDRAM voltage. • v5 - 5V sensor. This monitors fans and micro-processor core voltage regulator. • CPU sensor. This monitors CPU voltage and micro-processor core voltage.
Description	The description of the entity being monitored for voltage. Values are: • 2.5V voltage (millivolts) • 3.3V voltage (millivolts) • 5V voltage (millivolts) • CPU voltage (millivolts)
Current voltage (millivolts)	The current voltage measurement, in millivolts, if available. A value of -1 indicates that the monitor cannot obtain a value.

Name	Description
Sensor state	The current state of the voltage for the device being monitored. Values are: • Host Processor 7450 and 7455 • normal range: 1.55v to 1.65v • minor range: 1.4v to 1.55v or 1.65v to 1.8v • shutdown range: <1.4v or >1.8v • Host Processor 7457 • Version 1.0 • normal range: 1.35v to 1.45v • minor range: 1.00v to 1.35v or 1.45v to 1.6v • shutdown range: <1.0v or >1.6v • Version 1.1 and later • normal range: 1.25v to 1.35v • normal range: 1.25v to 1.35v • minor range: 1.00v to 1.25v or 1.35v to 1.6v • shutdown range: <1.0v or >1.6v
Slot ID	The slot on which this voltage is found.
Slot type	The type of module found in this slot.

View Temperature Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Environmental** performance group.
5. In the Environmental performance group pane, select the **Temperature** tab.
6. In the **Temperature** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Temperature source	The entity being monitored for temperature.
Description	A description of the temperature being monitored.
Current temperature (degrees Celsius)	The current temperature of the main board PROM in Celsius.

Name	Description
Sensor state	Current state of the temperature which can have one of the following values: • **initial**—The temperature is at its initial state. • **normal**—The temperature is normal. • **minor alarm**—The temperature is greater than or equal to 53 degrees Celsius and less than 63 degrees Celsius. • **major alarm**—The temperature is greater than or equal to 63 degrees Celsius and less than 73 degrees Celsius. • **critical alarm**—The temperature is greater than 73 degrees Celsius. • **shutdown**—The system should be shutdown immediately. • **not present**—The temperature sensor does not exist. • **not functioning**—The temperature sensor is not functioning properly. • **unknown**—Information cannot be obtained because of an internal error.
Slot ID	The slot on which this temperature is found.
Slot type	The type of module found in this slot.

View Fans Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Environmental** performance group.
5. In the Environmental performance group pane, select the **Fans** tab.
6. In the **Fans** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic, increasing number. When this number reaches the maximum value, the agent wraps the value back to 1.

Name	Description
Location	Location of the fan. Values are: • **left fan** • **middle fan** • **right fan**
Description	The description of the fan. Values are: • **fan 1** • **fan 2** • **fan 3**
Current speed (% or range)	The current fan speed percentage.
Fan state	The current fan speed state. Values are: • **initial**: fan speed is at its initial state • **normal**: fan speed is normal • **minor**: fan speed is between 75% and 90% of the full fan speed • **major**: fan speed is between 50% and 75% of the full fan speed • **critical**: fan speed is less than 50% of the full fan speed • **shutdown**: system should be shutdown immediately • **not present**: fan sensor does not exist • **not functioning**—The fan sensor is not functioning properly. • **unknown**—Information cannot be obtained due to an internal error.
Slot ID	The slot in which this fan is found.

View Power Supply Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Environmental** performance group.
5. In the Environmental performance group pane, select the **Power supplies** tab.
6. In the **Power supplies** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic, increasing integer. When it reaches the maximum value, the agent wraps the value back to 1.
Location	The location of the power supply. Values are: • Left power supply (A) • Right power supply (B)
Description	The description of the power supply. Values are: • Power supply (A) • Power supply (B)
State	The current state of the power supply. Values are: • **normal**—The power supply is normal. • **unknown**—The power supply sensor does not exist.

View Card Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Environmental** performance group.
5. In the Environmental performance group pane, select the **Cards** tab.
6. In the **Cards** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Type	The location of the phy card. Values are: • left phy card (Phy 0) • right phy card (Phy 1)
Description	Description of the phy card. Values are: • Phy 0 for the left phy card • Phy 1 for the right phy card
State	The current state of the phy card. Values are: • **normal**—The state of the phy card is normal. • **unknown**—The phy card is not present.

Realms

The following sections describe the realms performance group data that can be viewed for a Oracle Communications Session Element Manager device.

View Current Details Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Realms** performance group.
5. In the Realms performance group pane, select the **Current details** tab.
6. In the **Current details** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1
Name	The name of the realm for which the following statistics are being calculated.
Status	The current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction.
Inbound active	The number of current active inbound sessions.
Inbound active session rate	The current inbound session rate in CPS.
Outbound active sessions	The number of current active outbound sessions.
Outbound current sessions rate	The current outbound session rate in CPS.
Inbound admitted	The total number of inbound sessions during the period.
Inbound not admitted	The total number of inbound sessions rejected due to insufficient bandwidth.
Outbound admitted	The total number of outbound sessions during the period.
Outbound not admitted	The total number of outbound sessions rejected because of insufficient bandwidth.
Short sessions	The lifetime number of sessions whose duration was less than the configured short session duration.

View Average Period/State Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Realms** performance group.
5. In the Realms performance group pane, select the **Average Period/State** tab.
6. In the **Average Period/State** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic, increasing number. When this number reaches the maximum value, the agent wraps the value back to 1.
Name	The hostname of the realm for which the following statistics are being calculated
Status	The current status of the specified realm, which is expressed as INS, constraintsviolation, or callLoadReduction.
Inbound high current	The highest number of concurrent inbound sessions during the period.
Inbound average session rate	The average rate of inbound sessions during the period in CPS.
Outbound high current	Highest number of concurrent outbound sessions during the period.
Outbound average session rate	The average rate of outbound sessions during the period in CPS.
Max burst rate	The maximum burst rate of traffic measured during the period (combined inbound and outbound).
Total seizures	The total number of seizures during the period.
Total answered sessions	The total number of answered sessions during the period.
Answer/Seizure ratio	The answer-to-seizure ratio, expressed as a percentage.For example, a value of 90 would represent 90%, or .90.
Average latency	The average observed one-way signaling latency during the period in milliseconds.
Max latency	The maximum observed one-way signaling latency during the period in milliseconds.

View Monthly Minutes Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Realms** performance group.
5. In the Realms performance group pane, select the **Monthly Minutes** tab.
6. In the **Monthly Minutes** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic, increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1.
Realm name	The name of the realm for which the following statistics are being calculated.
Realm status	Current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction.
Minutes left	The number of monthly-minutes left in the pool per calendar month for a given realm.
Minutes rejected	The number of rejected calls due to monthly-minutes constraints exceeded.

View QoS Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Realms** performance group.
5. In the QoS performance group pane, select the **QoS** tab.
6. In the **QoS** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1.
Realm name	The name of the realm for which the following statistics are being calculated.
Realm status	The current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction.
Period average	The average QoS factor observed during the period.
Period maximum	The maximum QoS factor observed during the period.
Period exceeded major	The peg counts the number of times the major Rfactor threshold was exceeded during the period.
Total exceeded major	The peg counts the number of times the major Rfactor threshold was exceeded during the lifetime.
Period exceeded critical	The peg counts the number of times the critical Rfactor threshold was exceeded during the period.
Total exceeded critical	The peg counts the number of times the critical Rfactor threshold was exceeded during the lifetime.

SIP Session

The following sections describe the SIP performance group data that can be viewed for a Oracle Communications Session Element Manager device.

View Current SIP Session Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Click the **SIP session** performance group.
5. In the SIP session pane, the **Current** tab appears. The following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Hostname	The hostname of the SIP session agent for which the following statistics are being calculated.
Index	A number for the sole purpose of indexing session agents. When it reaches the maximum value, the agent wraps the value back to 1.
Statusad	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound current active sessions	The number of current active inbound sessions.
Inbound session rate	The current inbound session rate in the current performance session (CPS).
Outbound current active	The number of current active outbound sessions.
Outbound current session rate	The current outbound session rate in CPS.
Inbound admitted	Total number of inbound sessions during the period.
Inbound not admitted	Total number of inbound sessions rejected due to insufficient bandwidth.
Outbound admitted	Total number of outbound sessions during the period.
Outbound not admitted	Total number of outbound sessions rejected because of insufficient bandwidth.

View the Average Period and State of a Session

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Click the **SIP session** performance group.
5. In the SIP session performance group pane, select the **Average period/state** tab. The following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Hostname	The hostname of the session agent for which the following statistics are being calculated.
Index	The number for the sole purpose of indexing SIP session agents. When it reaches the maximum value, the agent wraps the value back to 1.
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound highest concurrent	The highest number of concurrent inbound sessions during the period.
Inbound average session rate	The average rate of inbound sessions during the period in current performance session (CPS).
Outbound highest concurrent	The highest number of concurrent outbound sessions during the period.
Outbound average session rate	The average rate of outbound sessions during the period in CPS.
Max burst rate	The maximum burst rate of traffic measured during the period (combined inbound and outbound).
Total seizures	The total number of seizures during the period.
Total answered	The total number of answered sessions during the period.
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90.
Average one-way signaling latency (ms)	The average observed one-way signaling latency during the period.
Maximum one-way signaling latency (ms)	The maximum observed one-way signaling latency during the period.

View Call Admission Control Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Click the **SIP session** performance group.

5. In the SIP session pane, select the **CAC** tab. The following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A number for the sole purpose of indexing SIP session agents. When it reaches the maximum value, the agent wraps the value back to 1.
Current session utilization level	The call admission control (CAC) utilization value for sessions of SIP session agents.
Current burst rate utilization level	The CAC utilization value for burst rate utilization of SIP session agents.
Object ID	(Hidden) The SNMP object ID for the SIP session agent.

H.323 Session

View Current H.323 Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **H.323 Session** performance group.
5. In the H.323 Session performance group pane, select the **Current** tab.
6. In the **Current** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Hostname	The hostname of the session agent for which the statistics are being calculated.
Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.

Name	Description
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound current active sessions	The number of current active inbound sessions.
Inbound session rate	The current Inbound Session rate in CPS.
Outbound current active	The number of current active outbound sessions.
Outbound current session rate	The current outbound session rate in CPS.
Inbound admitted	The total number of inbound sessions during the period.
Inbound not admitted	The total number of inbound sessions rejected due to insufficient bandwidth.
Outbound admitted	The total number of outbound sessions during the period.
Outbound not admitted	The total number of outbound sessions rejected because of insufficient bandwidth.

View Average Period/State Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **H.323 Session** performance group.
5. In the H.323 Session performance group pane, select the **Average period/state** tab.
6. In the **Average period/state** tab, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Index	A monotonic, increasing integer. When it reaches the maximum value the agent wraps the value back to 1.
Name	The hostname of the session agent for which the statistics are being calculated.

Name	Description
Status	The current status of the specified session agent, which is expressed as: • inService • outOfService • outOfServiceconstraintsviolation • BecomingoutOfService • ForcedoutOfService
Inbound high current	The highest number of concurrent inbound sessions during the period.
Inbound average session rate	The average rate of inbound sessions during the period in CPS.
Outbound high current	Highest number of concurrent outbound sessions during the period.
Outbound average session rate	The average rate of outbound sessions during the period in CPS.
Max burst rate	The maximum burst rate of traffic measured during the period (combined inbound and outbound).
Total seizures	The total number of seizures during the period.
Total answered	The total number of answered sessions during the period.
Answer/Seizure ratio (%)	The answer-to-seizure ratio, expressed as a percentage. For example, a value of 90 would represent 90%, or .90
Average latency	The average observed one-way signaling latency during the period.
Max latency	The maximum observed one-way signaling latency during the period.

NSEP

Use this performance group to view national security emergency preparedness (NSEP) data.

View National Security Emergency Preparedness (NSEP) Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **NSEP** performance group.
5. In the NSEP pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Current active sessions in	The number of current active inbound NSEP sessions.
Period high inbound	The highest number of concurrent inbound NSEP sessions during the period.
Total sessions in	The total number of inbound NSEP sessions during the period.
Period	The period for which the statistics are collected in seconds.
Current active sessions in	The number of current active NSEP sessions.
Total sessions in	The total number of inbound NSEP sessions during the period.
Period high in	The highest number of concurrent inbound NSEP sessions during the period.
Total not admitted	The total number of inbound NSEP sessions rejected.
Current active out	The number of current active outbound NSEP sessions.
Total sessions out	The total number of outbound NSEP sessions during the period.
Period high out	The highest number of concurrent outbound NSEP sessions during the period.
Total not admitted	The total number of outbound NSEP sessions rejected.

Trap Table Summary

View Trap Table Summary Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Trap table summary** performance group.
5. In the Trap table summary performance group pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Trap name	The trap name for this fault condition.
Number of variables	The number of variables encoded in the trap.

Name	Description
System uptime	The SNMP sysUptime when the trap was generated.

Storage Utilization

View Storage Utilization Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Storage utilization** performance group.
5. In the Storage utilization performance group pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Volume name	The name of the disk partition as defined by the user.
Total space (MB)	The total amount of disk space.
Available space (KB)	The free disk space that is available.

Intrusion Detection System (IDS)

View IDS Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **IDS** performance group.
5. In the IDS performance group pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
SIP endpoint demotions from trusted to untrusted	The global counters for SIP endpoint demotions from trusted to untrusted.
SIP endpoint demotions from untrusted to denied	The global counters for SIP endpoint demotions from untrusted to denied.
MGCP endpoint demotions from trusted to untrusted	The global counter for MGCP endpoint demotions from trusted to untrusted.
MGCP endpoint demotions from untrusted to denied	The global counters for MGCP endpoint demotions from untrusted to denied.

Cached Contacts

View Cached Contacts Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Cached contacts** performance group.
5. In the Cached contacts performance group pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
SIP local contacts	The number of active SIP local contacts.
MGCP GW endpoints	The number of MGCP GW endpoints.
H.323 registrations	The number of H.323 registrations.

Network Management Controls

View NM Control Data

1. Expand the **Performance Manager** slider and select **Devices**.

2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **NM controls** performance group.
5. In the NM controls performance group pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Name	The name of the network management (NM) control.
Type	The type of network management control.
Incoming total	The total number of incoming calls that match a destination identifier.
Rejected total	The total number of incoming calls that are rejected.
Diverted total	The total number of incoming calls that are diverted.
Incoming current	The number of incoming calls during the current period that match a destination identifier.
Rejected current	The number of incoming calls that are rejected during the current period.
Diverted current	The number of incoming calls diverted during the current period.
Incoming period max	The maximum number of incoming calls during a period that match a destination identifier.
Rejected period max	The number of the maximum incoming calls rejected in a period.
Diverted period max	The number of the maximum incoming calls diverted in a period.

ENUM Servers

View ENUM Servers Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **ENUM servers** performance group.

5. In the ENUM servers performance group pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Config name	The name of the ENUM configuration.
Server IP address	The IP address for the ENUM server.
Server status	The status of the ENUM server.

View Codec and Transcoding Data

Codec data displayed by Oracle Communications Session Element Manager is available for supported C-series and D-Series Oracle Communications Border Controller (SBC) products.

> **Note:**
>
> SBCs need to have a transcoding NIU card for Codecs to work.

View Codec Data

Codec data displayed by Oracle Communications Session Element Manager is available for supported C-series and D-Series Oracle Communications Border Controller (SBC) products.

> **Note:**
>
> SBCs need to have a transcoding NIU card for Codecs to work.

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **Codec** performance group.
5. In the Codec statistics pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Realm name	The realm that corresponds with the listed codec.
Other	The codecs that are not matched with the standard, well-known list of codecs.

> **Note:**
>
> All standard, well-known codecs are listed in the remaining columns.

CPU Core Table

View CPU Core Table Data

1. Expand the **Performance Manager** slider and select **Devices**.
2. In the **Devices** pane, navigate to the device group folder you want.
3. Select a device in the device group folder and click **View**.

   The **Performance Groups** folder appears in the navigation pane with performance groups below it.
4. Select the **CPU core** performance group.
5. In the CPU core performance group pane, the following information displays:

> **Note:**
>
> The information displayed in the performance group pane depends on your product device and its version, which may be different or more current than the information below. See your device product documentation for more information.

Name	Description
Core index	A monotonic, increasing integer for the sole purpose of indexing.
Description	The core ID and slot location.
CPU usage	The percentage of total CPU being used.
State	The current CPU state.
Memory descriptor	The type of RAM memory.
Memory usage	The current amount of RAM being used by the CPU.

7
Device Work Orders

You can use device work orders to configure automatic software upgrades and downgrades, or administer global configuration parameter changes across a targeted group of devices by creating a customized work order, assigning the devices, and applying these changes.

A device work order contains the following:

- Work order type—The software upgrade or global parameter changes.
- Targeted devices—The devices specified within the work order grouped by platform and software version.
- Work flow—A predefined work flow that defines the steps performed on the targeted devices, which is based on the type of work order you create for them.

Preparing for a Device Work Order

Complete the following applicable tasks before you configure a device work order.

User Permissions

The work order operations you can perform depend on the user permissions you are assigned. With the following user permissions assigned, you can perform operations relating to global software upgrades and global parameter changes:

- Administration: Create, modify, execute, delete and control a work order.
- Provision: Execute and control (start, abort, pause, resume, or commit) a work order.
- View: View work orders only.

High Availability Requirements

SFTP is required to support work order administration for Oracle Communications Session Element Manager clusters. Please ensure SFTP servers are running for Oracle Communications Session Element Manager servers.

Software Version Requirements

There is a software version requirement that applies under certain work order conditions:

- Global parameter changes: The software version of the global configuration must match the software version of the target devices.

If there are no devices selected in the work order's targeted device table, the Select SBC dialog box lists all of the devices managed by the Oracle Communications Session Element Manager server. However, once you add your first device to the Targeted devices table, the SBC dialog list adjusts to reflect only those devices with the same hardware type and software release version as the first device you added.

Software Image Archive Management

The software image archive allows you to view, load and delete all device software images maintained through Oracle Communications Session Element Manager. Before you create your work order, you must upload the correct software image to the software image archive.

You can add the software image to the archive through the Oracle Communications Session Element Manager Software image archive management table. If the targeted Oracle Communications Session Element Manager server is in a cluster, the Oracle Communications Session Element Manager server ensures that the new image is replicated for all nodes in a cluster.

To access the Software image archive management table, expand the Device Manager slider, followed by the Software upgrade folder. Click Software image archive management. From here you can view, add or delete software image files. The device software image archive directory is listed above the device software image table.

Software Downgrade Capability

There may be instances when you want to downgrade the software version for multiple devices. The procedure is virtually the same for a downgrade as for an upgrade. The difference is when you select your target software image, you choose a lower software version than the currently-running software version.

Provisioning a Device For Global Parameter Changes

A global configuration stores the configuration changes to be applied in your work order. The **Seeded from** parameter determines where the global configuration is seeded from.

Global configurations can be seeded from two options:

- Managed device—the configuration from the selected device is loaded to the global configuration. The configuration data model reflected on your screen are the elements required for that device's model, as well as the unique configuration values for the device's configuration.
- Software version—the data schema for a selected device software version model and default values are loaded to the global configuration. If you select this option, you must select a platform and software version. The available platforms and software versions depend on the devices managed by Oracle Communications Session Element Manager.

Best Current Practices

Global parameter changes require extensive validation across multiple devices simultaneously. For the highest success rate, it is recommended to implement global parameter change work orders across devices with similar configuration models.

Tracking Modifications in the LCV

Once you have created a global configuration, you must load the global configuration. Any modifications made to the global configuration schema are tracked in the Local Configuration View (LCV). Refer to Viewing Modifications in the LCV for instructions on how to view the LCV. For further information on modifications in the LCV, you can select an attribute and click **View Changes**.

The changes displayed in the LCV are additions, deletions, and modifications of top-level elements and/or sub-elements. For a detailed view of attribute modifictions, you can access the Preview screen. Refer to Viewing Attribute Parameters Modification and Elements Addition Deletion Tables for instructions on how to view element and attribute modifications, additions, and deletions.

Setting Criteria

You have to set the criteria for the multiple-instance elements you modified in your work order. Since some configuration elements occur more than once, you use the **Set Criteria** parameter to indicate which multiple-instance elements you want the changes applied to when you execute your work order.

> **Note:**
>
> Once you assign a global configuration to a work order, you can continue to update the global configuration. However, it is important to remember that you must set criteria for certain elements. You access the Set Criteria parameter through the work order, so you must ensure that this step is complete for executing your work order.

About Device Tasks

Device tasks are the individual tasks performed for each targeted device in the work order. The Device tasks table is found below the Work orders tables for both software upgrade and global parameter changes. Refer to the Device Tasks Table section for more information.

Work Order Provisioning Cycle

The following procedures are to serve as suggested methods. Your process might not follow these steps precisely.

Software Upgrade

This section provides an overview of performing a software upgrade.

1. Upload the target software image to the software image archive. Refer to Adding Software Images to the Software Image Archive Directory for more information.
2. Create a software upgrade work order. Refer to Creating a Software Upgrade Work Order for more information.
3. Name the work order.
4. Schedule start time, or leave blank to start manually. Refer to Scheduling Work Order Start Date and Time for more information.
5. Set the error policy, behavior, and auto-commit. Refer to Configuring the Error Policy, Configuring the Behavior, and Enabling Auto Commit for more information.
6. Add targeted devices. Refer to Adding Targeted Devices for more information.
7. Specify the target software image. Refer to Configuring Target Software Image for Software Upgrades for more information.

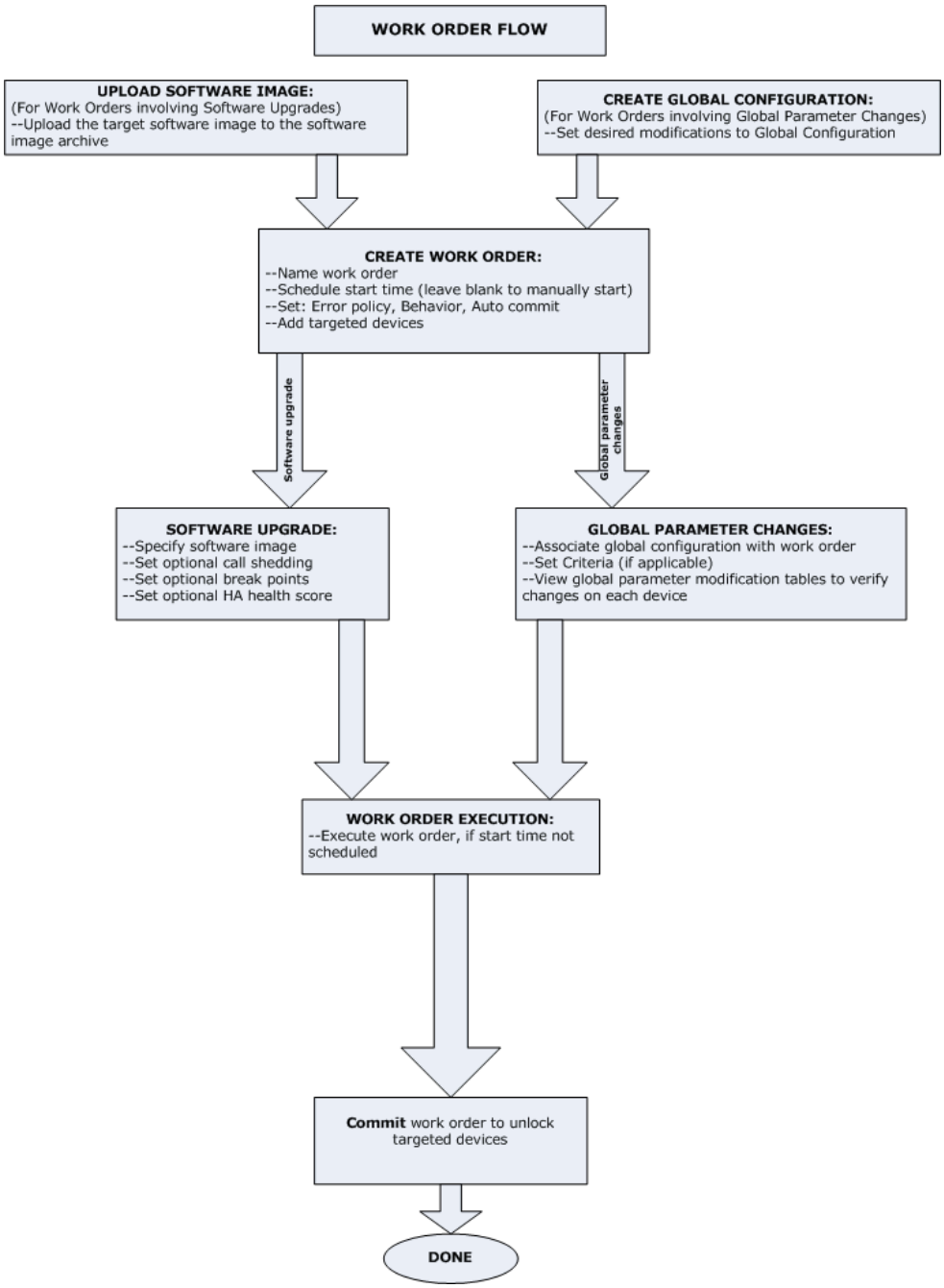
8. Set optional parameters, such as call shedding, break points, and HA health score. Refer to Configuring Optional Software Upgrade Parameters for more information.
9. Execute the work order. Refer to Executing a Work Order on Demand for more information.
10. Commit the work order. Refer to Commiting a Work Order for more information.

Global Parameters Changes

This section provides an overview of performing global parameter changes.

1. Create a global configuration. Refer to Creating Global Configurations for more information.
2. Set modifications to your global configuration.
3. Create a global parameter changes work order. Refer to Creating a Global Parameter Changes Work Order for more information.
4. Name the work order.
5. Schedule start time, or leave blank to start manually. Refer to Scheduling Work Order Start Date and Time for more information.
6. Set the error policy, behavior, and auto-commit. Refer to Configuring the Error Policy, Configuring the Behavior, and Enabling Auto Commit for more information.
7. Add targeted devices. Refer to Adding Targeted Devices for more information.
8. Assign a global configuration to the work order. Refer to Assigning the Global Configuration to the Work Order for more information.
9. Set criteria for multiple-instance elements (if applicable). Refer to Setting Criteria for Element Instances in Work Orders for more information.
10. View global parameter modification tables to verify changes on each device. Refer to Modifications Tables for more information.
11. Execute the work order. Refer to Executing a Work Order on Demand for more information.
12. Commit the work order. Refer to Commiting a Work Order for more information.

    The following diagram illustrates the work order flow.



Work Order Administration Graphical User Interface

Software upgrade and global parameters changes work orders are created and maintained in separate sliders.

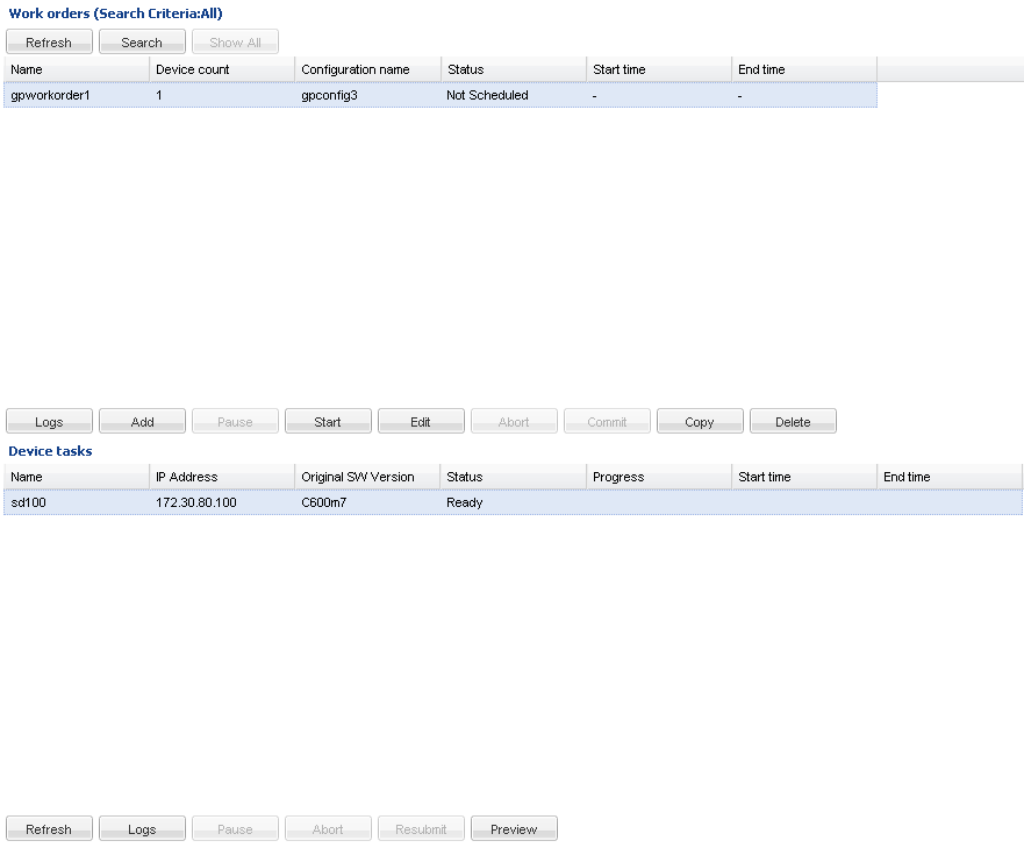
You access the software upgrade work order administration in the Device Manager slider. You access the global parameter changes work order administration in the Configuration Manager slider. Refer to the Performing a Software Upgrade or Performing Global Parameter Changes sections for instructions.

The Work order view, available in the Dashboard Manager, allows you to view all work orders. You can also access device tasks tables here. However, this is a read-only view.

In their respective work order tables, you create new work orders, delete any unused work orders, and perform other functions described in the work order actions table below.

Work Order Table

Below is the global parameter changes Work orders table. First, we will review the portions of work order administration that are the same for software upgrades and global parameters changes.



Accessing Work Order Tables

1. To access the software upgrade work order table, expand the **Device Manager slider** > **Software upgrade**, and click Work order administration.
2. To access the global parameter changes work order table, expand the Configuration Manager slider, click Global parameters, and click the Admin tab at the top of the content area.

Work Order Table Actions

You can perform the following actions for both software upgrade and global parameter changes unless noted. The buttons are disabled (or grayed out) when an action cannot be performed at a particular time.

Action	Description
Logs	Launches the work order log.
Refresh	Causes the Oracle Communications Session Element Manager to retrieve the work orders from the server and display the most current status.
Add	Launches the Create/Edit work order view.
Pause	Waits for the currently-running task to stop gracefully, putting the work order in a paused state.
Start	Starts unscheduled work order immediately, restarts a work order, or resumes a a work order, depending on the work order state.
View/Edit	The availability of these actions vary depending on the state of the work order. View launches the Create/Edit work order view in read-only mode; no configuration changes are possible. Edit launches the Create/Edit work order view for editing purposes; a work order cannot be modified if its state is scheduled, running, stopped, success, or failed.
Abort	Aborts the work order.
Commit	Manually commits a selected work order. The targeted devices are unlocked once a work order is committed. Only work orders with statuses of: Success, failed, abort, or abortFailed can be committed.
Copy	Duplicates an existing work order configuration and puts the work order in a partially-configured state. You have to modify the copy of the work order before it can be executed.
Delete	Deletes the selected work order from the Oracle Communications Session Element Manager database. The Oracle Communications Session Element Manager will never automatically delete a work order, even when the work order has successfully completed. A work order can only be deleted if its status is PartialConfigured, NotScheduled, or Committed.

Work Order Table Data

Data	Description
Name	Name you give the work order.
Type	This column is only available if viewing in the Dashboard Manager. Type of the work order: SW Upgrade GP Changes
Device count	Number of targeted device nodes (standalone devices or HA pairs) the work order will execute. An HA pair is considered one device node.
Configuration Name	For global parameter changes only: Global configuration name applied in this work order.
Target SW version	For software upgrades only: The software version to be installed.

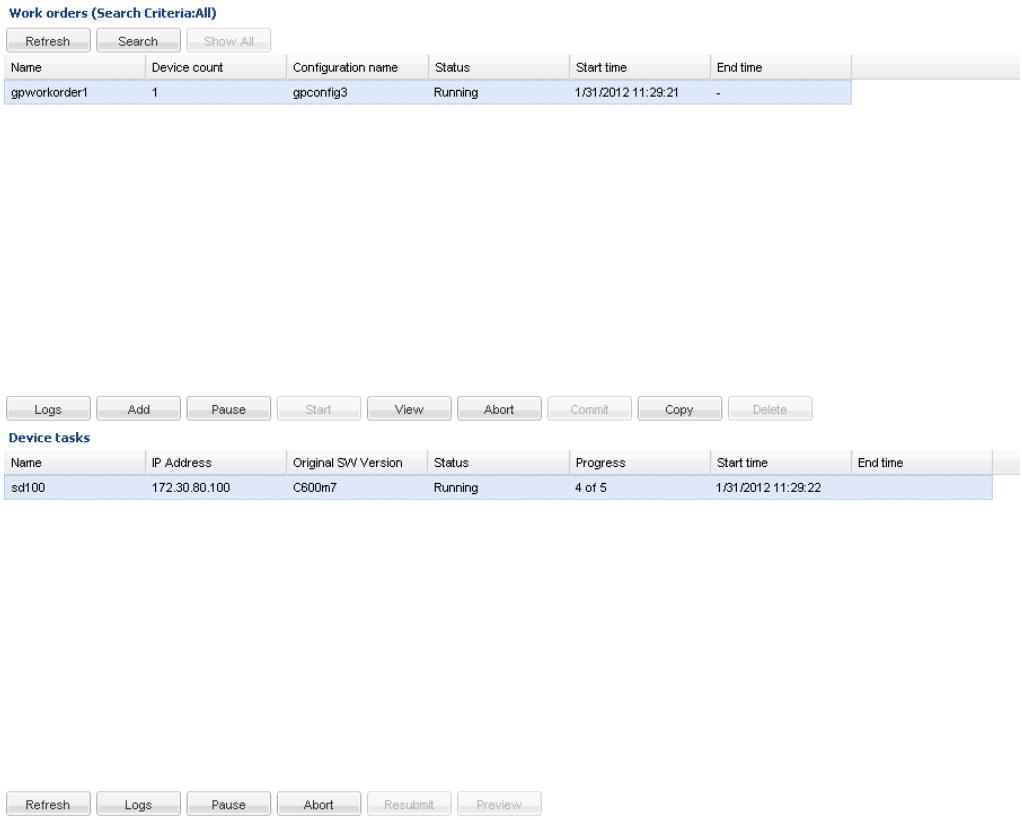
Data	Description
Status	The possible statuses of the work order: PartiallyConfigured: Configuration is incomplete. NotScheduled: Start time is not yet configured. Scheduled: The start time is configured and scheduled to begin at a set date and time. WaitStarting: Work order is placed into a run-waiting queue by the Oracle Communications Session Element Manager scheduler and awaits the scheduled time to start running. Running: Work order started and is currently processing. Pausing: Work order pauses after Pause is initiated by user. Paused: Work order stopped completely. You must manually resume a stopped task or abort the task. Resuming: Work order resumes processing. Success: Work order completed successfully, but has not yet been committed. Failed: Work order failed during execution. StartCommitting: Work order is in the StartCommitting state. Committing: Work order is in the process of committing the changes designated. Committed: Changes successfully executed by this work order are committed CommitFailed: Work order failed to commit and some of the locked resources or the auto-generated files may fail to remove. StartAborting: Work order is in the beginning process of aborting. Aborting: Work order is executing the abort process. Aborted: Work order has been successfully aborted. All changes made on all targeted devices are rolled back and the devices retain their original state prior to the work order execution. AbortFailed: Work order failed to abort due to a failure of a device rollback process. Preloading: This status applies to software upgrades only. The state the work order is in when the Pause and unlock after loading software image parameter is enabled in the software upgrade configuration, and the work order is loading the target software image to all targeted devices. PreloadPause: This status applies to software upgrades only. This state occurs after the work order successfully delivered the target software image to the targeted devices and unlocked the devices. You can resume the work order in this state. PreloadFailed: Work order failed to load the target software image to all targeted devices. LockingResource: State when the work order locks all necessary resources. LockResourceFailed: Work order failed to lock all necessary resources. You can restart the work order in this state.
Start time	The Oracle Communications Session Element Manager server start date and local time for this work order.

Data	Description
End time	The end time is the Oracle Communications Session Element Manager local time when: The work order finished successfully and paused. A failed condition has been met and the work order stopped as a result of the failure. The user manually stops a work order already in progress.

The following table defines the data displayed in the Work orders table:

Device Tasks Table

Below the Work orders table is the Device tasks table. Device tasks are the individual tasks performed for each targeted device in the work order.



Device Task Actions

The following table lists the actions available for device tasks. You must select a device task row in order to execute any of these actions.

Action	Description
Refresh	Oracle Communications Session Element Manager retrieves the device tasks from the server and display the most current status.
Logs	Launches the device tasks log.
Pause	Waits for the currently-running task to stop gracefully, putting the device task in a paused state.
Abort	Aborts the device task.
Resubmit	The work order is resubmitted to start excecution from the start of the work flow for the targeted device node.
Preview	This button is only available for global parameter changes. Opens the Configuration table and Attributes modification table.

Device Task Data

The following table lists the data that pertains to device tasks.

Data	Description
Name	Name of the targeted device which can be a standalone device or an HA pair.
IP address	device management IP address. For HA pairs, the IP addresses for each device appear.
Original SW version	Original software image for this device.

Data	Description
Status	Status of an individual task: Ready: Ready to run. ResetToReady: When a work order is resubmitted, all failed tasks are reset to this state to distinguish it from the initial Ready state. Starting: An intermediate state between the Ready and Running states when you submit or resubmit the device task. Running: Task has begun and is running. Pausing: An intermediate state between Running and Paused states. Paused: Task was stopped completely. A paused task must be resumed manually, or aborted. Success: Task has completed execution successfully. Failed: Task has failed to complete. StartAborting: A task starts to abort. Aborting: A task is executing the rollback procedure and you manually abort the procedure, or the device task automatically rolls back due to an error during the procedure. Aborted: Rollback procedure is successful. AbortFailed: A task does not successfully rollback and failure occurs. Preloading: A task is loading the target software image to the device. PreloadPaused: A task has loaded the target software image to the device and is paused. PreloadFailed: A task failed to load the target software image to the device.
Progress	Total number of procedural steps completed for this device task. For example, 12/12 indicates 12 steps have completed in a 12-step process within a work order scenario.
Start time	Oracle Communications Session Element Manager local time that the device task is scheduled to start, or the time when a task within the work order has started. If the work order has not reached its scheduled start time, all individual tasks for this work order will display the same start time. When an individual task begins, the processing start time replaces the scheduled time.
End time	Oracle Communications Session Element Manager local time when: Work order finished successfully and stopped. Failed condition has been met and the work order stopped as a result of the failure. User manually stops a work order already in progress.

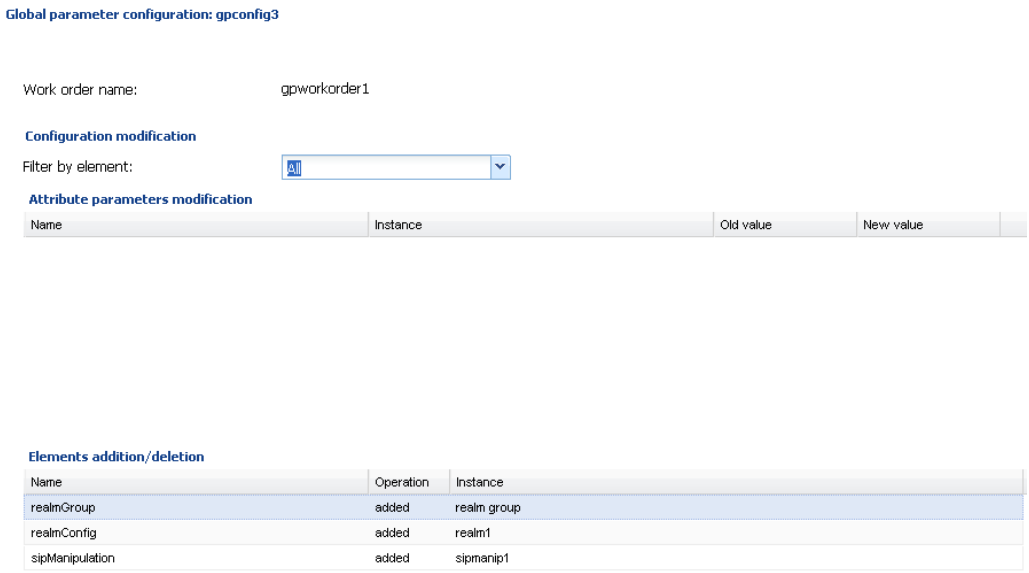
Configuration and Attributes Modification Tables

The Attribute parameters modification and Elements addition/deletion tables are only available for global parameter changes, and display the top-level element, sub-element, and attribute modifications.

The **Filter by element** drop-down parameter allows the user to view the configuration changes by element type.

To open these tables, select a device task and click **Preview**.

See Viewing Attribute Parameters Modification and Elements Addition Deletion Tables for instructions to access these tables.



Attribute Parameters Modification Table Data

The following table lists the data that pertains to attribute parameters modifications.

Data	Description
Name	The name of the changed parameter. The syntax is element-type/attribute-name.
Instance	String value of the key for to identify the specific instance.
Old value	Old parameter value configured for this parameter.
New value	New parameter value configured for this parameter.

Elements addition/deletion Table Data

The following table describes the data available in the Elements addition/deletion table**.**

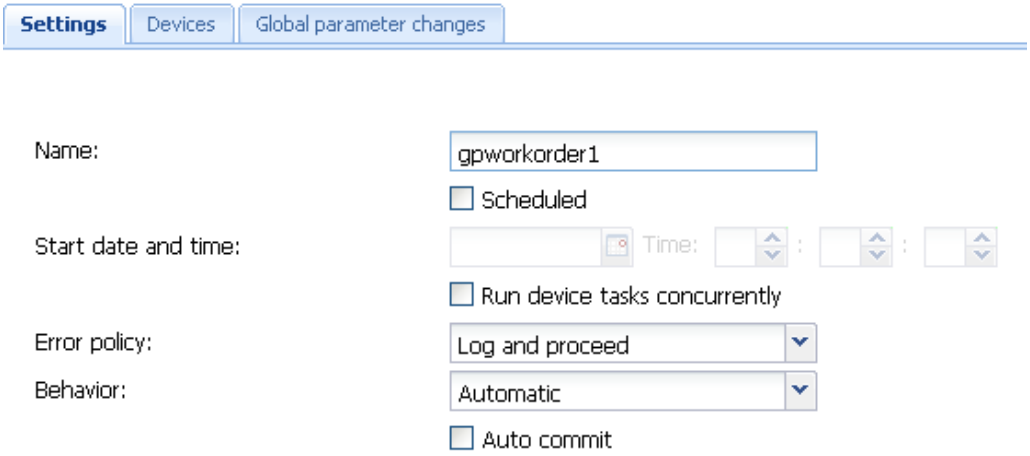
Data	Description
Name	The name of the element type which is going to be added or deleted.
Instance	String value of the key to identify the specific element instance.
Operation	Operation performed on this element: Add: This element was added to this global configuration. Delete: This element was deleted from this global configuration.

Work Order Settings and Devices Tabs

Work orders are comprised of three tabs containing required parameters. For software upgrade and global parameter changes work orders, the first two tabs are the same: Settings and Devices. The third tab is unique for each work order: Workflows tab for software upgrades, and Global parameter changes tab for global parameter changes. The unique tabs are discussed in further detail in their respective GUI sections below.

Settings Tab

The Settings tab contains parameters for naming, scheduling and committing the work order.



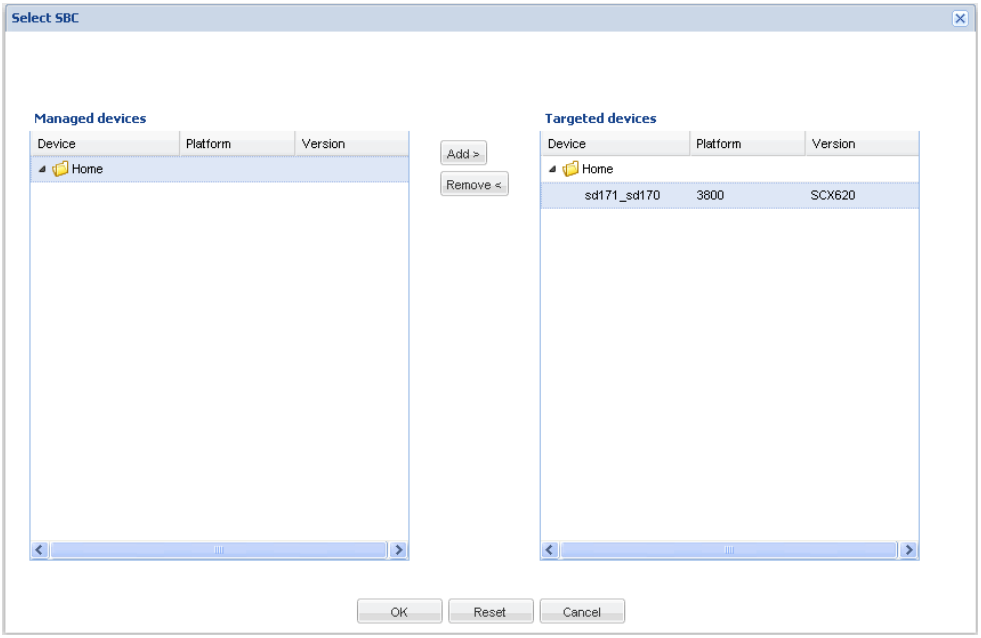
For more information on configuring these parameters, please consult the Work Order Administration section.

Devices Tab

The Devices tab allows you to select targeted devices for your work order.

Before you select devices, it is important to note the following:

- Once you select a device from the Managed devices table and add it to the Targeted devices table, only devices with the same software version remain in the Managed devices table.
- When selecting devices for a global parameter changes work order, the global configuration assigned to the work order must match the software version of the targeted devices.

- 

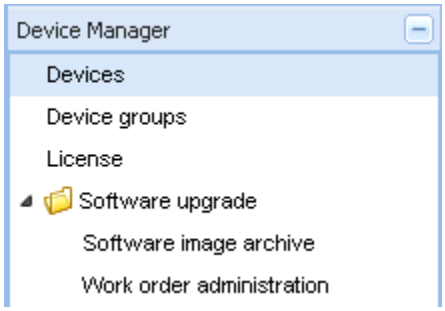
For more information on configuring these parameters, please consult the Adding Targeted Devices section.

Software Upgrade Work Order Administration

Now we will discuss elements that are unique to software upgrade work order administration.

To access software upgrade work order administration:

1. Expand the **Device Manager slider** > **Software upgrade**.
2. Click Work order administration.

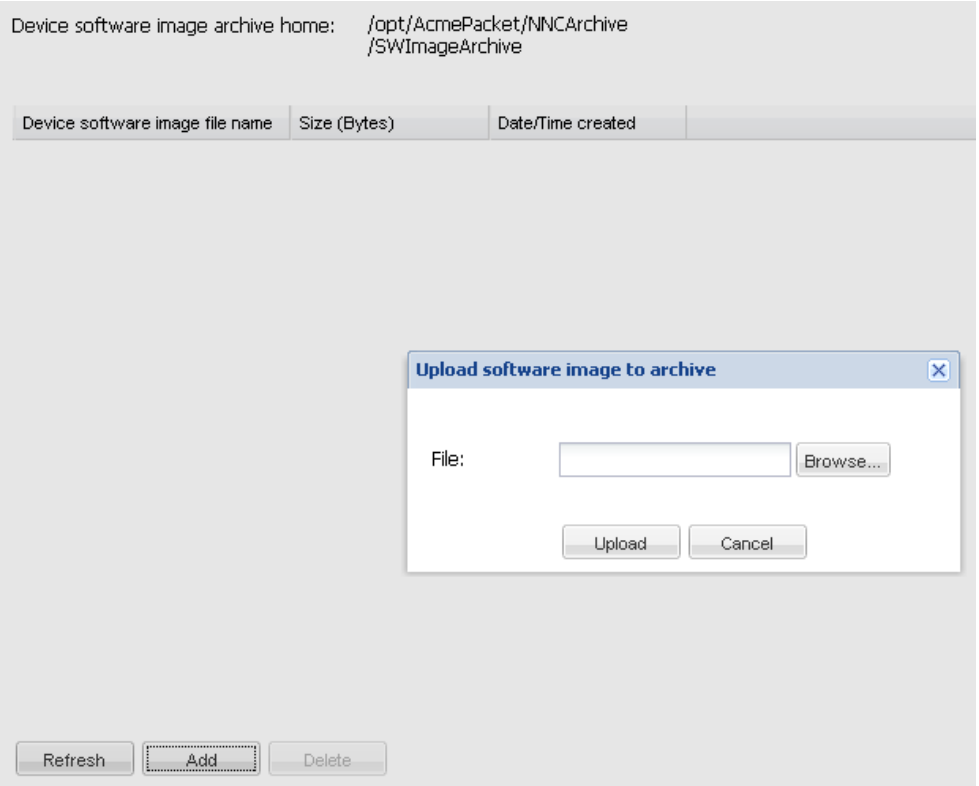


Software Image Archive

To access software upgrade work order administration:

1. Expand the Device Manager slider > Software upgrade.
2. Click Software image archive.

   Below is the screen for uploading software images to the archive. For instructions, please refer to Adding Software Images to the Software Image Archive Directory.



Software Image Archive Management Data

The following information is displayed on the Software image archive screen:

Data	Description
Device software image archive home	The directory the software image files are uploaded to.
Device software image name	Name of the device software image.
Size (Bytes)	Size of the software image file in Bytes.
Date	Date and time when the file was stored to the disk.

Software Image Archive Management Actions

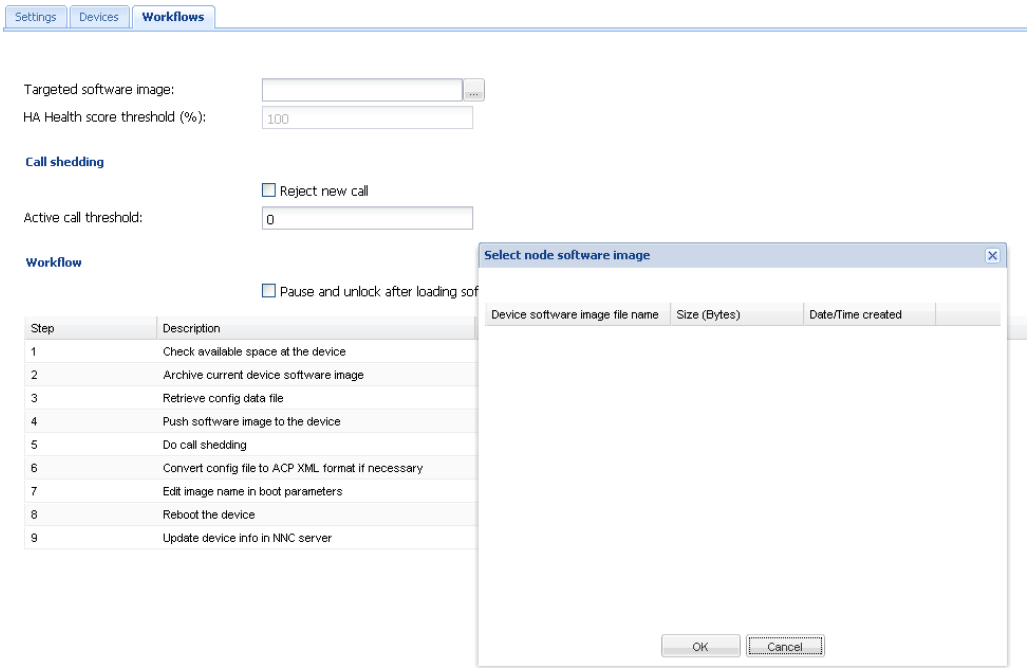
The software archive management action buttons allow you to:

Action	Description
Refresh	Refreshes the software image file data.
Delete	Manually deletes the selected software image file from the archive home directory.
Cancel	Closes the work order administration window.

Work Order Administration

There are three tabs containing required parameters for work order administration. Below is the Workflows tab, which is unique to software upgrades. Please refer to Work Order Settings and Devices Tabs for more information on the Settings and Devices tabs.

The Workflows tab allows you to select the targeted software image, set a health score threshold for HA pairs, enable call shedding and set pause breaks after steps in the predefined work flow for work orders. For instructions, please consult Configuring Optional Software Upgrade Parameters.



Global Parameter Changes Work Order Administration

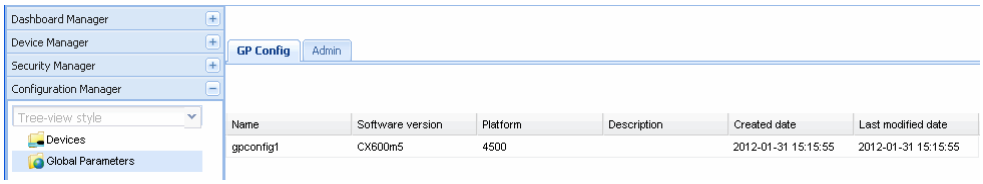
Now we will discuss elements that are unique to global parameter changes work orders. Before you create a global parameter changes work order, you must create a global configuration to store your configuration modifications.

Accessing Global Configuration Table

To access the global configuration table:

1. Expand the Configuration Manager slider.
2. Click Global parameters.
3. Click the GP Config tab at the top of the content area.

   Below is the Configuration Manager slider before loading a global configuration, and a portion of the GP Config table in the content area.

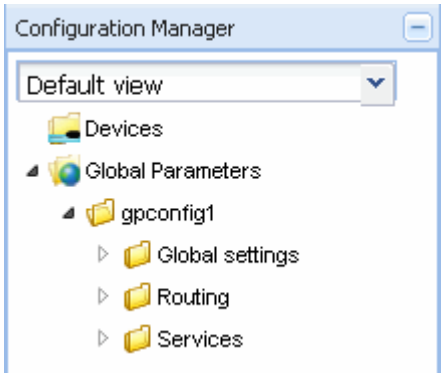


Loading a Global Configuration

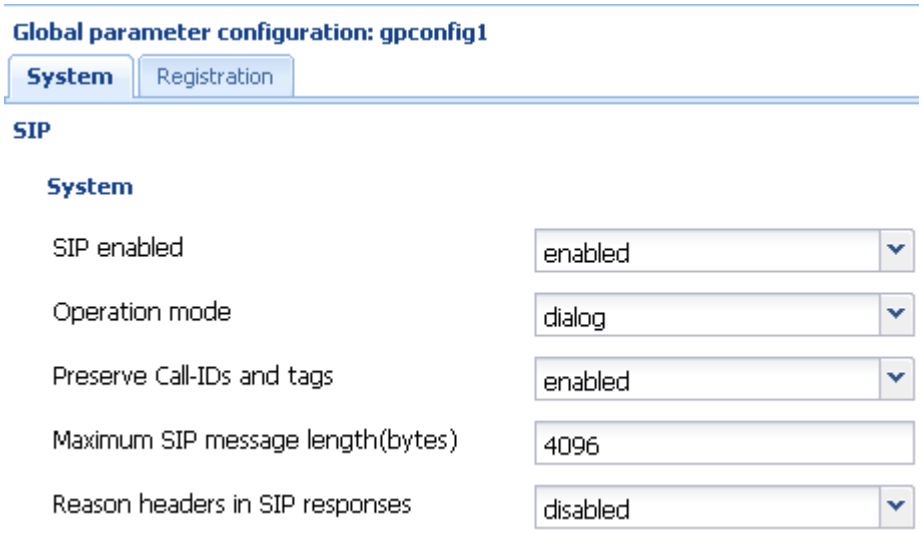
To load a global configuration:

1. Select a global configuration from the table and click **Load**.

   Once you load a global configuration, the global configuration name appears below the Global parameters icon. Any configurations made under this folder will be contained in the global configuration, and applied to targeted devices through a work order.



The global configuration name also appears at the top of the content area when it is loaded.



GP Config Tab Actions

The following table lists the actions available for the global configuration table.

Action	Description
Refresh	Oracle Communications Session Element Manager retrieves the global configurations from the server and displays the most current status.
Add	Launches the Create global configuration screen in the content area.
Edit	Allows you to edit the name and description of this global configuration.

Action	Description
Load	Load the selected global configuration for storing global parameter changes.
View changes	Launches the Local Configuration View (LCV) for this global configuration.
Delete	Deletes the selected global configuration.

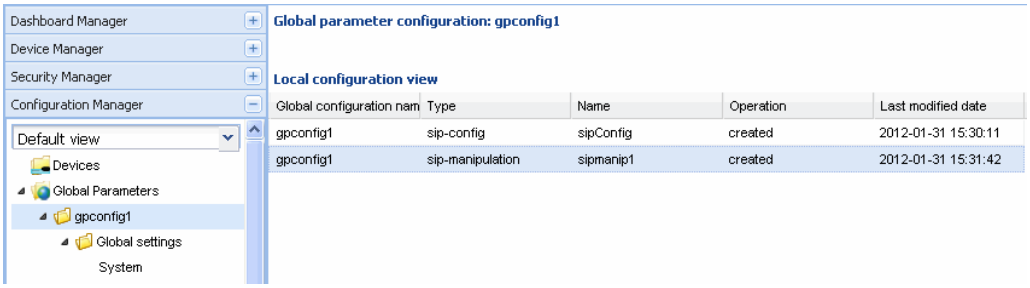
GP Config Tab Data

The following table lists the data pertaining to the global configuration table.

Data	Description
Name	The name of this global configuration.
Software version	The software version used to seed this global configuration. The targeted devices in your work order must match this software version.
Platform	The platform used to seed this global configuration. The targeted devices in your work order must match this software version.
Description	The unique description for this global configuration.
Created date	The date this global configuration was created.
Last modified date	The last date this global configuration was modified.

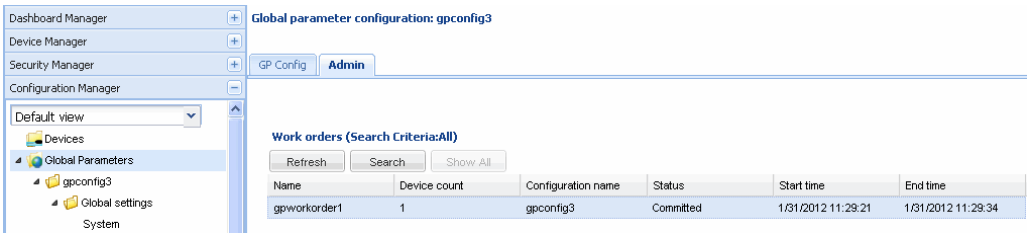
Local Configuration View (LCV)

The local configuration view lists the elements created, deleted or modified by the user. This list is organized by element type. Sub-elements are listed by their parent element. Please consult Viewing Modifications in the LCV for instructions on accessing the LCV. For a more detailed preview of modifications for targeted devices, refer to the Attribute parameters modifications table (Viewing Attribute Parameters Modification and Elements Addition Deletion Tables.

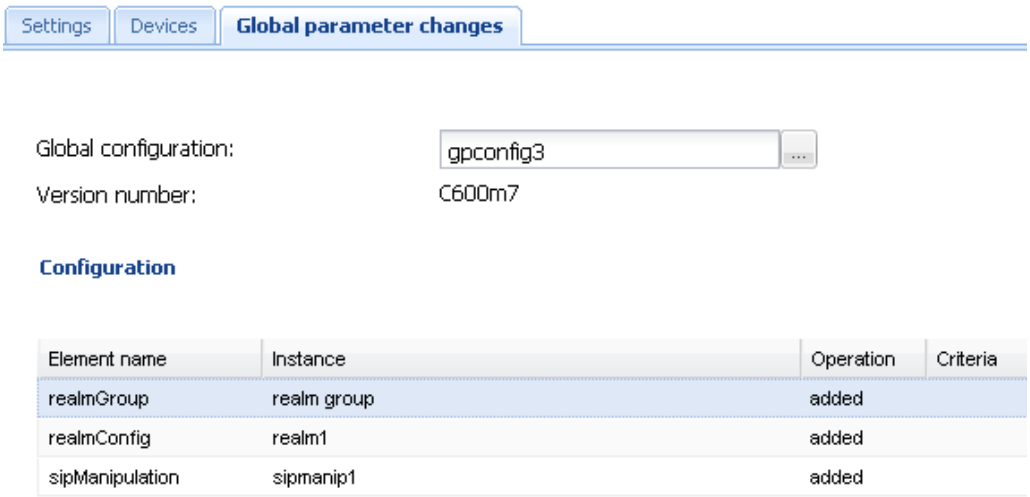


Work Order Administration

To access the global parameter changes work order administration, you must click the Admin tab.



You can click the **Add** button in the Work orders table to create one, or select an existing work order and click **Edit**; both options will open the Work order administration tabs. There are three tabs containing required parameters for work order administration. Below is the Global parameter changes tab, which is unique to global parameter change work orders. Please refer to Work Order Settings and Devices Tabs for more information on the Settings and Devices tabs.

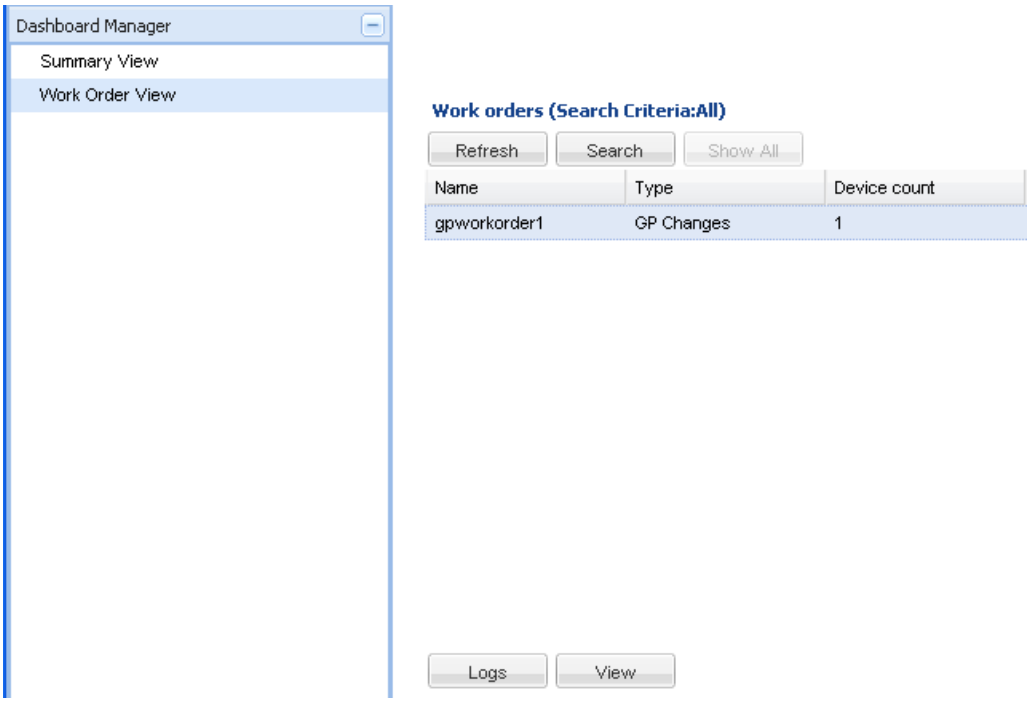


Once you have selected targeted devices in the Devices tab, only global configurations seeded from the same software version are available in the Global configuration parameter.

Please consult Creating a Global Parameter Changes Work Order for instructions on creating a global parameter changes work order.

Work Order View

Below is the Dashboard Manager slider, and a portion of the Work Order View screen.



The only actions available through this view are:

Action	Description
Logs	View work order logs.
View	View launches the Create/Edit work order view in read-only mode; no configuration changes are possible.

Performing a Software Upgrade

The following procedures show you how to create a work order to perform a software upgrade across a group of targeted devices. If necessary, you load your target software image to the software image archive directory in the Software Image Archive screen of the Device Manager slider. For more information, see the Adding Software Images to the Software Image Archive Directory section.

Once you load the proper images, you can create your software upgrade work order and configure corresponding parameters. Next, you pick the targeted devices you want to upgrade and select the target software image. Finally, you set optional call shedding, break points, and an HA health score (applicable to HA pairs only). These optional parameters are discussed in further detail in Configuring Optional Software Upgrade Parameters.

Adding Software Images to the Software Image Archive Directory

One image is required for a software upgrade: the software image to be installed in the upgrade.

To add a software image to the software image archive directory:

1. Expand the **Device Manager slider** > **Software upgrade**.
2. Click Software image archive.

3. Click **Add**. The Upload software image to archive dialog box appears.
4. Select the image file from the File Upload dialog box.
5. Click **Open**.
6. Click **Upload**. The image now appears in the table.

Creating a Software Upgrade Work Order

To create a software upgrade work order:

1. Expand the Device Manager slider > Software upgrade.
2. Click Work order administration.
3. In the Work orders table, click **Add**.The content area opens to the Settings tab of work order administration.
4. **Name**—Enter the descriptive name you want to give this work order. The name must be an alphanumeric value from 1 to 24 characters in length. The name must be unique.

> **Note:**
>
> You have completed required configuration for the work order settings. You cannot apply these changes until you have selected devices in the Devices tab, and selected a target software image in the Workflows tab.

For more information on parameters in the Settings and Devices tab, see the Work Order Administration section.

5. Click the Devices tab at the top of the content area.
6. Click **Add** at the bottom of the content area. The Select SBC dialog box appears.
7. Expand the folders from Managed devices table and select a device to highlight it.
8. Click **Add** to move the device to the Selected devices table.

> **Note:**
>
> Work orders are limited to one platform and software version at a time. Once you select your first device and add it to the Selected devices table, only devices with the same platform and software version remain in the Managed devices table.

9. Repeat steps 6 through 8 to add additional targeted devices. To add multiple targeted devices at one time, hold the **Ctrl** key while you click each device.
10. Click **OK**. The devices appear in the targeted devices table.

> **Note:**
>
> You have completed required configuration for the work order devices tab. You cannot apply these changes until you have selected the target software image in the Workflows tab.

Configuring Target Software Image for Software Upgrades

This procedure is required for all software upgrades.

To configure the target software image for a software upgrade:

1. Click the Workflows tab at the top of the content area.
2. **Targeted software image**—Click  to open the Select SBC software image dialog box.
3. Select the targeted software image in the Select SBC software image table that you want to upgrade to.
4. Click **OK**.
5. Click **Apply** in the Workflows content area. The newly created software upgrade work order appears in the Work orders table.

Configuring Optional Software Upgrade Parameters

You can configure optional parameters within the software upgrade work order to pause at certain points during the work order process. There are two optional pause settings you can choose from, enabling the **Pause and unlock after loading software image** parameter and/or inserting break points.

Below is a summary of optional parameters for software upgrade parameters:

Data	Description
Target software image	Software image you are upgrading to.
Pause and unlock after loading software image	(Optional) The work order is paused after the software image is delivered to all targeted devices. The targeted devices are unlocked once the software is successfully delivered.
Break points	(Optional) An intentional stoppage of the work order. When you insert a break point, the work order is stopped after the step preceding the break point successfully completes. You must manually resume the work order.
Call shedding	(Optional) During the software upgrade process, the device will not be rebooted with the new image until the call threshold is reached.
Set HA health score	(Optional) Set a health score threshold value for HA pairs only.

Configuring Pause and Unlock After Loading Software Image

When the optional **Pause and unlock after loading software image** parameter is enabled, the work order is paused after the software image is delivered to all targeted devices. The targeted devices are unlocked once the software is successfully delivered. The work order can be later resumed, and the devices reboot with the new images.

To configure pause and unlock after loading software image:

1. Select the work order you want to configure and click **Edit**.

2. Click the Workflows tab at the top of the content area.
3. **Pause and unlock after loading software image**—Click the checkbox to enable the preload pause state for software upgrade work orders. The default is **disabled**.
4. Click **Apply**.

Configuring Break Points

You can set optional break points after any step during the work order processing. A break point is an intentional stoppage of the work order. When you insert a break point, the work order is stopped after the step preceding the break point successfully completes. You must manually resume the work order.

To configure break points:

1. Select the work order you want to configure and click **Edit**.
2. Click the Workflows tab at the top of the content area.
3. **Pause after**—Click the checkbox in the Pause after column next to the step in the Step table to initiate a pause after this step completes successfully. You can insert as many breakpoints as you want. The default is unchecked, or **disabled**. The table describes:
   - Step—The number of this task in the work flow order
   - Description—Description of the task associated with this step
   - Pause after—When checked, enables a break point after this step has successfully completed. The default is **disabled**.
4. Click **Apply**.

Configuring Call Shedding

You can configure optional call shedding for a standalone device. When call shedding is enabled, the device reboots when the active-call threshold reaches its limit during the software upgrade process. You can check the performance management MIB to view the current call-shedding count. For more information about the performance management MIB, refer to the Oracle Communications AP4000 MIB Reference Guide.

To configure call shedding:

1. Select the work order you want to configure and click **Edit**.
2. Click the Workflows tab at the top of the content area.
3. Scroll to the **Call shedding** section.
4. **Reject new calls**—Click the checkbox to enable call shedding, whereby the device rejects new calls during the software upgrade process. The default is **disabled**.
5. **Active call threshold on SBC**—Enter the threshold number of active calls below which the upgrade/downgrade reboot proceeds automatically.
6. Click **Apply**.

Configuring a Health Score for HA Pairs Only

You can set a health score threshold value for HA pairs. During the software upgrade process, Oracle Communications Session Element Manager checks the health score to determine if the devices are in a stable condition.

> **Note:**
>
> If the health score value is set, and the device health is not above the health score value, the software upgrade will not proceed.

Once a new health score value is set, it is displayed in the work flow description check. By default the health score is set to 100%.

To configure the health score threshold for HA pairs:

1. Select the device work order you want to configure and click **Edit**.
2. Click the Workflows tab at the top of the content area.
3. **HA Health score threshold (%)**—Enter the health score percentage for this HA pair from 1 to 100 percent.
4. Click **Apply**.

Configuring Force Switchover to Restore Original HA Setup

You can restore the original HA pair active/standby configuration during the software upgrade process by enabling Force switchover to restore original HA setup. This option is disabled by default.

1. Expand the Device Manager > Software upgrade and click Work Order Administration.
2. Click **Add** or select an existing work order from the table and click **Edit**.
3. Click the Workflows tab.
4. **Force switchover to restore original HA setup if it is configured**— Click the checkbox to enable this feature.
5. Click **Apply**.

Setting the Behavior of Work Orders

6. Expand the Device Manager > Software upgrade and click Work Order Administration.
7. Click **Add** or select an existing work order from the table and click **Edit**.
8. Click the Settings tab.
9. **Force switchover to restore original HA setup if it is configured**— Select **Pause only after 1st device** from the combination box.
10. Click **Apply**.

Executing Work Order

Once your work order is created and your configuration is applied, you are ready to execute. You perform this step if you are manually executing your work order. Otherwise, your work order will execute at the date and time you set.

To manually execute your work order:

1. Refer to Executing a Work Order on Demand for information to perform this procedure.

Committing Work Order

Once your work order is executed, you must commit your work order to unlock all targeted devices associated with your work order.

To commit your work order and unlock all targeted devices associated with your work order:

1. Refer to Commiting a Work Order for information to perform this procedure.

Performing Global Parameter Changes

The following procedures show you how to create a work order to perform global parameter changes across a group of targeted devices. Before you create your global parameter changes work order, you must create a global configuration. The global configuration stores the global parameter changes you create for your work orders. Once you create a global configuration, you must load it to begin configuring. All global parameter changes must belong to a global configuration. You can create multiple global configurations, each containing global parameter changes for various hardware platforms and software versions. Please refer to the Provisioning a Device For Global Parameter Changes section for more information.

You have to set the criteria for the multiple-instance elements you modified in your work order. Since some configuration elements occur more than once, you use the **Set Criteria** parameter to indicate which multiple-instance elements you want the changes applied to when you execute your work order. For more information and instructions, please see the Setting Criteria for Element Instances in Work Orders section for more information.

In the following configuration example, we will create a work order to perform global parameter changes on one targeted device.

Creating a Global Configuration

When performing global parameter changes, you must create a global configuration, which becomes part of your work order. The global configuration is a device configuration that is a general purpose container for holding your configuration changes. The software version of the global configuration must match the software version of the targeted devices.

You create and/or modify the global configuration with the parameter changes you want applied to your targeted devices. Once the global configuration is assigned to your work order, the configuration attributes are sent to the targeted devices when the work order is executed.

Global configurations can be seeded from two options:

- Managed device—the configuration from the selected device is loaded to the global configuration. The configuration data model reflected on your screen are the elements required for that device's model, as well as the unique configuration values for the device's configuration model.
- Software version—the data schema for a selected device software version model and default values are loaded to the global configuration. If you select this option, you must select a platform and software version. The available platforms and software versions depend on the devices managed by Oracle Communications Session Element Manager.

Creating Global Configurations

To create a global configuration:

1. Expand the Configuration Manager slider.
2. Click Global Parameters.
3. Click the GP Config tab at the top of the content area.
4. In the GP Config table, click **Add**.
5. **Configuration name**—Enter the name you want to give to this global configuration. The name must be an alphanumeric value from 1 to 24 characters in length. The name must be unique.
6. **Description**—Enter a description for this global configuration.
7. **Global configuration seeded from**—Select the global configuration option from the drop-down list.
   - Managed device—the configuration from the selected device is loaded to the global configuration. The configuration data model reflected on your screen are the elements required for that device's model, as well as the unique configuration values for the device's configuration.
   - Software version—the data schema for a selected device software version model and default values are loaded to the global configuration. If you select this option, you must select a platform and software version. The available platforms and software versions depend on the devices managed by Oracle Communications Session Element Manager.

     If you select Managed device, the Software version parameters are disabled, and you must select a managed device.

     If you select Software version, the Managed device parameter is disabled, and you must select a platform and supported software version.
8. **Platform**—Available only if you select Software version for the **Global configuration seeded from** parameter. Select the device hardware platform of the targeted devices.
9. **Supported software version**—Available only if you select Software version for the **Global configuration seeded from** parameter. Click the software version of the device you want to use for your default global configuration in the drop-down list.
10. **Managed device**—Available only if you select Managed device for the **Global configuration seeded from** parameter. Select the managed device you want to use for your global configuration base.
11. Click **Apply**. The global configuration now appears in the GP Config table.

Modifying Global Parameters

To modify global parameters, you must load the global configuration and begin configuring.

To make global configuration changes:

1. Expand the Configuration Manager slider and click Global parameters.
2. Click the GP Config tab at the top of the content area.
3. Select a global configuration from the table and click **Load**. A Success dialog box appears to confirm that the global configuration has successfully loaded.
4. Click **OK**. The global configuration name now appears below the Global Parameters icon in the slider, as well as at the top of the content area.

5. Expand configuration folders in the Configuration Manager slider to access configuration elements and sub-elements.
6. Make changes to your global configurations as you would a single device. Please see the Oracle Communications Session Element Manager Configuration Guide for instructions on configuration.

> **Note:**
>
> Each time you apply configuration changes in your global configuration, the modifications are added to the database. They are not provisioned to your device until you execute and commit your work order. The LCV logs additions, deletions, and modifications of top-level elements.

Viewing Modifications in the LCV

To view configuration modifications for your global configuration:

1. Click the Global parameters icon in the Configuration Manager slider.
2. Click the GP Config tab at the top of the content area, and select and global configuration.
3. Click **View Changes**.
4. The Local configuration view table appears in the content area and displays the top-level element changes for this global configuration.
5. You can select a top-level element and click **View Detail** for further attribute modification details.

Viewing Attribute Parameters Modification and Elements Addition/ Deletion Tables

To preview attribute parameter modifications and element addition/deletions:

1. Click Global parameters in the Configuration Manager slider.
2. Click the Admin tab at the top of the content area.
3. Select a work order in the Work orders table and the device tasks for this work order will populate in the Device tasks table.
4. Select a device task for your work order from the table.
5. Click **Preview**. The Attribute parameters modifications and Element addition/deletions tables for the selected device appear in the content area.

   For more information on this table, please consult Preview Screen in the Troubleshooting and Logs section.

Creating a Global Parameter Changes Work Order

You create your work order after creating your global configuration. The modifications you made to your global configuration are assigned to your work order and are applied to the targeted devices in the work order.

To create a global parameter changes work order:

1. Expand the Configuration Manager slider.
2. Click Global parameters.
3. Click the Admin tab at the top of the content area.
4. In the Work orders table, click **Add**. The content area opens to the Settings tab of work order administration.
5. **Name**—Enter the descriptive name you want to give this work order. The name must be an alphanumeric value from 1 to 24 characters in length.

   You have completed configuration for the work order settings. You cannot apply these changes until you have selected devices in the Devices tab, and selected a global configuration in the Global parameter changes tab.

   > **Note:**
   >
   > For more information on parameters in the Settings and Devices tab, see Work Order Administration.

6. Click the Devices tab at the top of the content area.
7. Click **Add** at the bottom of the content area. The Select SBC dialog box appears.
8. Expand the folders from Managed devices table and select a device to highlight it.
9. Click **Add** to move the device to the Targeted devices table.

   > **Note:**
   >
   > Work orders are limited to one platform and software version at a time. Once you select your first device and add it to the Selected devices table, only devices with the same platform and software version remain in the Managed devices table.

10. Repeat steps 7 through 9 to add additional targeted devices. To add multiple targeted devices at one time, hold the **Ctrl** key while you click each device.
11. Click **OK**. The devices appear in the targeted devices table.

    You have completed the required configuration for the work order Devices tab. You cannot apply these changes until you have selected a global configuration in the Global parameter changes tab.

Assigning the Global Configuration to the Work Order

To assign the global configuration in the work order:

1. Click the Global parameter changes tab at the top of the content area.
2. **Global configuration**—Click  to select your global configuration. The Select global configuration dialog box appears.
3. Select the global configuration you want to assign to this work order and click **OK**.

   The **Global configuration** parameter populates with the global configuration and the **Version number** parameter populates with the software version for this global configuration.

4. If you have criteria to set, do not click **Apply** and proceed to the next section.
5. If you do not have criteria to set, click **Apply**. A Success dialog box appears after your work order is updated.
6. Click **OK**. The Work orders table appears.

   From here you set the criteria for multiple-instance elements that you want to change when you execute your work order.

Setting Criteria for Element Instances in Work Orders

You have to set the criteria for the multiple-instance elements you modified in your work order. Since some configuration elements occur more than once, you use the **Set Criteria** parameter to indicate which multiple-instance elements you want the changes applied to when you execute your work order.

Setting criteria means selecting which instances of a configuration record type the modifications should be applied to on your targeted devices. For example, if you modify a parameter for a session agent, you set the criteria to indicate which session agents within this targeted device you want to modify when your work order is executed.

By enabling the **Apply changes to all instances** parameter, you can set the criteria for all instances of a multiple element at once.

> **Note:**
>
> Once you assign a global configuration to an unscheduled work order, you can continue to update the global configuration. However, it is important to remember that you must set criteria for certain elements. You access the Set Criteria parameter through the work order, so you must ensure that this is complete for executing your work order.

The criteria syntax you enter must follow one of these rules:

- Exactly match the specified instance. The instance is specified by using whatever “key” attribute values are appropriate for that type of configuration element. For example, in the case of a session agent the key is hostname.
- The system prompts you for input strings for each criteria.

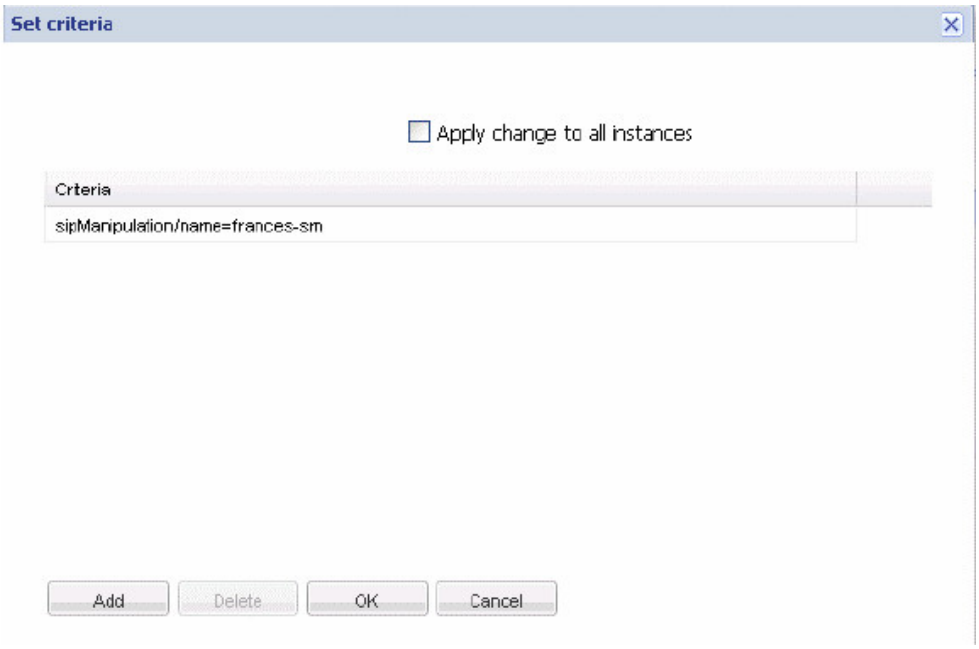
Set criteria is **disabled** for system-wide elements since there is only one instance for a system-wide element and no criteria is needed.

Configuring Element Criteria

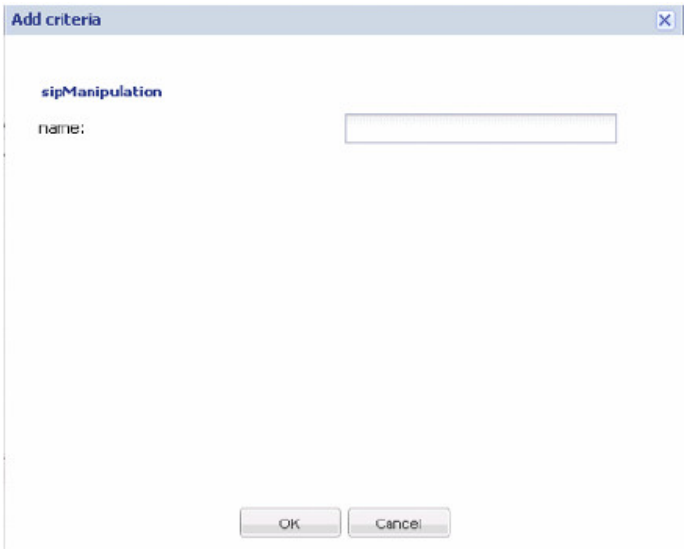
To set the criteria for an element in the work flow configuration:

1. Click Global parameters in the Configuration Manager slider.
2. Click the Admin tab at the top of the content area to access the Work orders table.
3. Select the work order which contains the global configuration for which you would like to set criteria. The Configuration Name column of the table lists the global configurations.
4. Click **Edit**.
5. Click the Global parameters changes tab.
6. Click the Element name you want to set criteria for in the Configuration table.

7. Click **Set criteria**. The Set criteria dialog box appears.



8. Click **Add**. The Add criteria dialog box appears. (For this example, the primary key for a SIP manipulation is name. The Add criteria text field references the ACLI attribute name.) The element instance is dynamic and changes depending on the type of element instance you are setting criteria for.



Note:

The Add criteria dialog box automatically prompts you for all attributes that make up the primary key for the selected type of configuration element.

9. Enter the specific criteria needed. For example, realmid

> **Note:**
>
> You must know which values are considered valid for the particular attribute you are setting criteria for.

10. Click **OK**. The criteria is added to the Criteria column of the Configuration table.
11. **Apply changes to all instances—**Click the checkbox to apply the criteria to all instances of this multiple element.
12. Click **OK**.
13. To set multiple criteria instances, repeat steps 6 through 12.
14. Click **Apply**. Your work order is updated successfully.

    If you click **Apply** when you have not set the criteria instances you will get an error message.
15. Click **OK** to clear the message.

Viewing Set Criteria Details

To view set criteria:

1. From the Edit work order window, click the element you want to view in the Configuration table.
2. Click **Set criteria** beneath the configuration table. The criteria for the element you selected appears in the Set criteria window.

Executing Work Order

Once your work order is created and your configuration applied, you are ready to execute your work order. You perform this step if you are manually executing your work order. Otherwise, your work order will execute at the date and time you set.

To manually execute your work order:

1. Refer to Executing a Work Order on Demand for more information to perform this procedure.

Committing Work Order

Once your work order is executed, you must commit your work order to unlock all targeted devices associated with your work order.

To commit your work order and unlock all targeted devices associated with your work order:

1. Refer to Commiting a Work Order for information to perform this procedure.

Work Order Administration

The following parameters are configured for both software upgrade work orders and global parameter changes work orders. These procedures assume that you have created a work order

and are ready to begin configuring. See the Creating a Software Upgrade Work Order or Creating a Global Parameter Changes Work Order sections for instructions. This section also provides instruction for executing and committing both types of work orders. When the **Run device tasks concurrently** parameter is enabled, the **Error policy** and **Behavior** parameters are set to "Log and Proceed" and Automatic, respectively, by default. These values cannot be changed in that instance.

Scheduling Work Order Start Date and Time

This is an optional parameter. You can execute your work order on demand, or you can schedule it to start at a specified date and time.

To schedule the start date and time:

1. In the Settings tab, click the **Scheduled** checkbox. Leave this checkbox blank if you want to execute your work order on demand.
2. **Start date and time**—Click  to access the Calendar.
3. Select the month and the year by using the arrows. The down arrow beside the month and year allows you to select any month and year. The left and right arrows allow to navigate to the previous or next month.
4. Select the day by clicking the appropriate cell.
5. **Time**—Select the hour, minute and second by typing the numbers in the text box or using the arrows.

Configuring the Error Policy

The error policy you configure determines how errors are handled when they occur during the execution of your work order. The **Error policy** parameter is set to Log and Proceed when the **Run device tasks concurrently** parameter is enabled.

To configure the error policy:

1. **Error policy**—Select the error policy from the drop-down list that you want to apply to this work order. You can choose:
   - Log and proceed (default)—The targeted device that experienced the error will be rolled back to its original configuration state and the work order will proceed to the next targeted device in the work order list
   - Stop—The targeted device that experienced the error will be rolled back to its original configuration state and the work order will stop. You must manually resume, or abort, the work order
   - Stop and rollback—All targeted devices processed up to the time of the error will be rolled back to their original configuration states and the work order will stop

Configuring the Behavior

You configure the behavior you want to apply to this work order. The **Behavior** parameter is set to Automatic when the **Run device tasks concurrently** parameter is enabled.

To set the behavior:

1. **Behavior**—Select the work order behavior you want to apply to this work order from the drop-down list. The two types of behaviors are:
   - Automatic (default)—The software upgrade or global parameter changes proceeds on each targeted device without requiring intervention
   - Device-level—The software upgrade or global parameter changes pause after each targeted device finishes updating. You must manually continue on to the next targeted device listed in the work order

     If an error occurs during the work order execution, the behavior is controlled by the error policy.

Enabling Auto Commit

This is an optional parameter. When a work order has completed, but has not yet been committed, it retains a lock on all its targeted devices. This means that no other operations can be performed on those devices. Once a work order is committed, the devices associated with the work order are unlocked. If you enable auto commit, your work order will be automatically committed after execution. Only work orders with a success status are automatically committed. The default is **disabled**. When **disabled**, you must manually commit the work order from the work order administration window to unlock the devices associated with it.

Until you commit, you have the opportunity to abort this work order and perform a rollback to restore the original software version and/or original configuration settings.

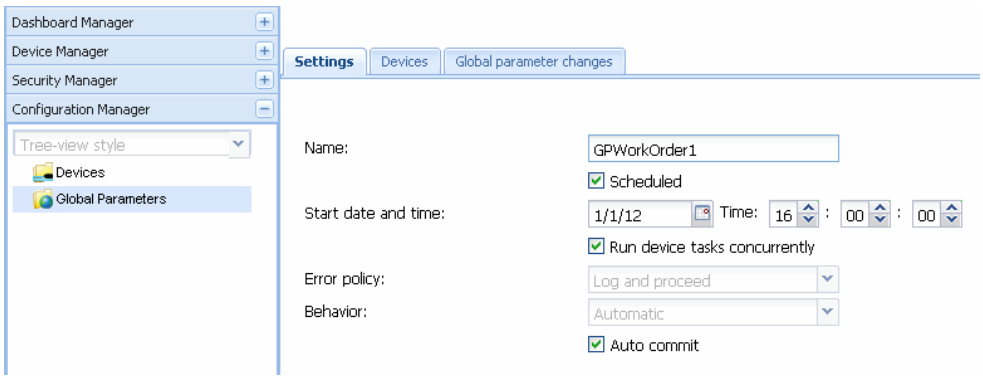
To enable auto commit:

1. **Auto commit**—Click the check box to enable auto commit for this work order. The work order will be automatically committed after execution.

   > **Note:**
   >
   > Once a work order is committed, rollback is no longer possible. When you commit a work order, all targeted devices associated with this work order are unlocked.

2. Click **Apply**.

   You have completed configuration for the work order settings. You cannot apply these changes until you have selected devices in the Devices tab, and selected a target software image for a software upgrade in the Workflows tab, or a global configuration for a global parameter change in the Global parameter changes tab.



Adding Targeted Devices

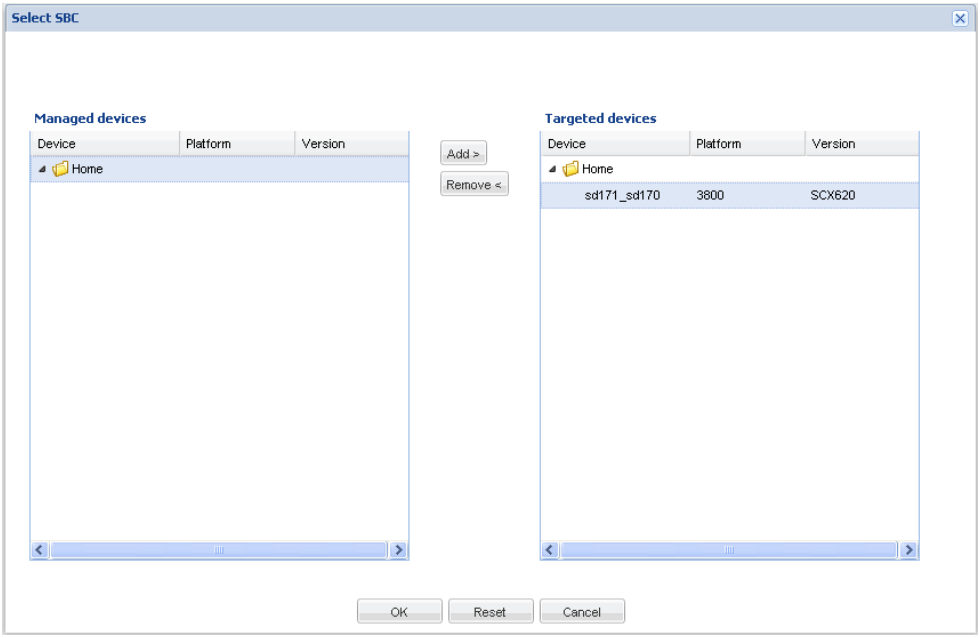
You add the targeted devices you want to apply to your work order.

To add targeted devices to your work order:

1. Click the Devices tab at the top of the content area.
2. Click **Add** at the bottom of the content area. The Select SBC dialog box appears.
3. Expand the folders from Managed devices table and select a device to highlight it.
4. Click **Add** to move the device to the Selected devices table.

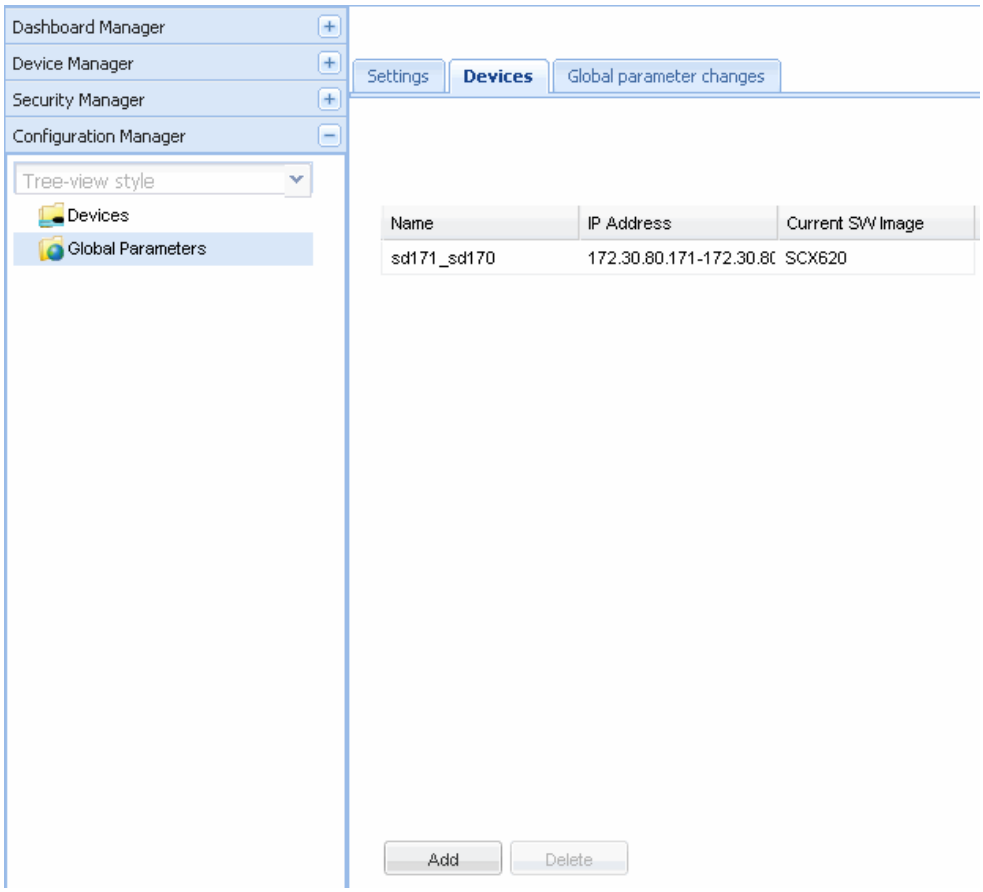
> **Note:**
>
> Work orders are limited to one platform and software version at a time. Once you select your first device and add it to the Selected devices table, only devices with the same platform and software version remain in the Managed devices table.

5. Repeat steps 12 and 13 to add additional targeted devices. To add multiple targeted devices at one time, hold the **Ctrl** key while you click each device.



6. Click **OK**. The devices appear in the targeted devices table.

   You have now added targeted devices. You cannot apply these changes until you have selected a target software image for a software upgrade in the Workflows tab, or a global configuration for a global parameter change in the Global parameter changes tab.



7. Please proceed to the section Creating a Software Upgrade Work Order or Creating a Global Parameter Changes Work Order to complete work order configuration.
8. Once you have completed work order administration, click **Apply** at the bottom of the content area.

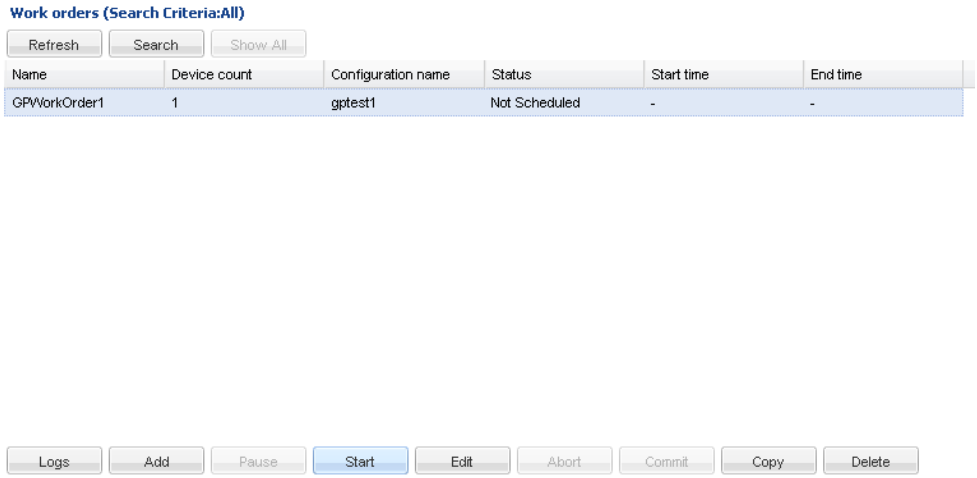
   If you set the time for a period that has passed, you will get an error message when you click **Apply**. Click **OK** to close the message, and click the Settings tab to correct the error.

Executing a Work Order on Demand

The following procedure is universal to all work order types and must be performed to execute your work order (unless you have scheduled a start date and time for your work order to begin processing).

To execute your work order on demand:

1. Perform one of the following sets of steps to access the proper Work orders table:
   - Software upgrade—Expand the Device Manager slider followed by the Software upgrade folder. Click Work order administration.
   - Global parameters changes—Expand the Configuration Manager slider and click Global parameters. Click the Admin tab at the top of the content area.
2. Select the work order you want to execute.



3. Click **Start**. A confirmation message appears.
4. Click **Yes**.
5. Click **Refresh** to confirm the Status changes from Not Scheduled to Running.

Commiting a Work Order

After you execute a work order, it must be committed in order to unlock the targeted devices associated with it. Only work orders with a status of Success, Failed, Aborted, AbortFailed, or CommitFailed can be committed. When you commit a work order, rollback is no longer possible, and all targeted devices associated with this work order are unlocked. This work order can no longer be modified. You must create a new work order to implement new changes.

You can automatically commit your work order. By enabling the **Auto commit** parameter, the work order is automatically committed after a successful execution. The default is **disabled**. When disabled, you must manually commit the work order. Refer to Enabling Auto Commit for more information about **Auto commit**.

Until you commit, you have the opportunity to abort this work order and perform a rollback to restore the original software version and/or original configuration settings.

Manually Committing a Work Order

To manually commit a work order:

1. Expand the Device Manager slider> Software upgrade.
2. Click Work order administration.
3. Select the work order you want to commit and click **Commit**. A confirmation dialog box appears.
4. Click **Yes**.
5. Click **Refresh** to confirm the work order status changed from Success to Committed.

Pausing a Work Order

If you configure optional pause breaks for software upgrades, the work order changes to the Paused state. The work order Status and the device task Status is paused. You must resume the work order to resume executing the work order.

Resuming a Paused Work Order

To resume a paused work order:

1. Select the paused work order from the Work orders table.
2. Click the work order you want to resume and click **Resume**. A confirmation message appears.
3. Click **Yes**.
4. Click **Refresh** to confirm the status changed from paused to running.

   A success status appears when the work order completes successfully.

Predefined Work Flows

Each type of work order contains a predefined work flow that defines the execution procedure sequentially in a step-by-step process. As the work order is executed, the procedural step is tracked in the Device tasks table, under the Progress column. The steps are found in the Device tasks table, under the Progress column. The steps for each type of work-order scenario are defined in the tables below.

> **Note:**
>
> The rollback procedural steps listed below are based on the full rollback procedures when rolling back a successfully-executed device task. The rollback procedural steps may vary if the rollback process is initiated when a work order fails or is aborted during the execution process.

Software Upgrade for a Standalone Device

This table defines the procedural steps for a software upgrade involving a standalone device.

Step	Description
1	Checks available space for the device.
2	Archives the current device software image.
3	Retrieves running configuration data file for backup.
4	Pushes the software image to the device.
5	Performs call shedding.
6	Converts the configuration file to ACP XML format if necessary.
7	Edits the image name in the boot parameters.
8	Reboots the device.
9	Updates the device information in the Oracle Communications Session Element Manager server.

Software Upgrade for an HA Pair

This table defines the procedural steps for a software upgrade involving an HA pair.

Step	Description
1	Checks available space for both devices.
2	Checks status and health for both devices.
3	Archives the current device software image.
4	Retrieves running configuration data file for backup.
5	Pushes the software image to both devices.
6	Converts the configuration file to ACP XML format if necessary.
7	Edits the image name in the boot parameters for the standby device.
8	Reboots the standby device.
9	Checks the health of the standby device.
10	Forces a failover,and the standby device becomes the active device.
11	Edits the image name in the boot parameters for the new standby device.
12	Reboots the new standby device.
13	Updates the device information in Oracle Communications Session Element Manager server.

Software Rollback for a Standalone Device

This table defines the procedural steps for a software rollback involving a standalone device.

Step	Description
1	Pushes files to the device.
2	Performs call shedding.
3	Edits the image name in the boot parameters.
4	Reboots the device.
5	Updates the device information in Oracle Communications Session Element Manager server.

Software Rollback for an HA Pair

This table defines the procedural steps for a software rollback involving an HA pair.

Step	Description
1	Pushes the files to both devices.
2	Retrieves status and health score from both devices.
3	Edits the image name in the boot parameters from the standby device.
4	Reboots the standby device.
5	Performs switchover to standby device.
6	Edits the image name in the boot parameters from the standby device.
7	Reboots the new standby device.
8	Updates the device information in Oracle Communications Session Element Manager server.

Global Parameter Changes for a Standalone Device or an HA Pair

This table defines the procedural steps for global parameter changes involving a standalone device or an HA pair.

Step	Description
1	Checks the status of the device.
2	Retrieves the running configuration data file.
3	Loads the configuration from the device.
4	Creates configuration change set based on the global parameter changes.
5	Saves and activates the targeted device configuration on the device.

Global Parameter Changes Rollback for a Standalone Device or an HA Pair

This table defines the procedural steps for a rollback of global parameter changes involving a standalone device or an HA pair.

Step	Description
1	Checks the status of the device.
2	Pushes the original running configuration back to the device.
3	Restores the backup configuration on the device.
4	Saves and activates the configuration on the device.
5	Updates the device information in Oracle Communications Session Element Manager server.

Work Order Processing States and User Actions Matrices

Depending on the Oracle Communications Session Element Manager internal processing state of your work order, there are some actions you can perform during these states and some you cannot. The internal processing state is associated with the predefined process flow for each of the work order types. The actions in the work orders table and the device tasks table are dynamically enabled or disabled based on the state of the selected work order, or on a device task within the work order. The matrices below chart the various work order states and the actions you can or cannot perform when the work order is in a particular state. A warning dialog box will appear if you attempt an action that is not allowed during a state. Below are two matrices, one for work orders and one for device tasks.

Matrix for Work Order States and Actions

The matrix below details work order states and the actions you can perform during one of these states.

States Below:	Action: Edit	Action: Delete	Action: Copy	Action: Commit	Action: Abort	Action: Start	Action: Restart	Action: Resume	Action: Pause
Partially-Configured	Yes	Yes	Yes	No	No	No	No	No	No
NotScheduled	Yes	Yes	Yes	No	No	Yes	No	No	No
Scheduled	No	No	Yes	No	Yes	Yes	No	No	No
WaitStarting	No	No	No	No	Yes	Yes	No	No	No

States Below:	Action: Edit	Action: Delete	Action: Copy	Action: Commit	Action: Abort	Action: Start	Action: Restart	Action: Resume	Action: Pause
Running	No	No	No	No	Yes	No	No	No	Yes
Paused	No	No	No	No	Yes	No	No	Yes	No
Success	No	No	Yes	Yes	Yes	No	No	No	No
Failed	No	No	Yes	Yes	Yes	No	Yes	No	No
Committed	No	Yes	Yes	No	No	No	No	No	No
CommitFailed	No	No	Yes	Yes	No	No	No	No	No
Aborted	No	No	Yes	Yes	No	No	No	No	No
AbortFailed	No	No	Yes	Yes	Yes	No	No	No	No
PreloadPaused	No	No	No	No	Yes	No	No	Yes	No
Preloading	No	No	No	No	No	No	No	No	No
PreloadFailed	No	No	Yes	No	No	No	Yes	No	No
ResourceLocking	No	No	No	No	No	No	No	No	No
ResourceLockFailed	No	Yes	Yes	No	No	No	Yes	No	No

Matrix for Device Task States and Actions

The matrix below details device task states and the actions you can perform during one of these states.

States Below:	Action: Pause	Action: Resume	Action: Abort	Action: Submit	Action: Resubmit
Ready	No	No	No	Yes	No
ResetToReady	No	No	No	No	Yes
Running	Yes	No	Yes	No	No
Paused	No	Yes	Yes	No	No
Success	No	No	Yes	No	No
Failed	No	No	Yes	No	Yes
Rolledback	No	No	No	No	Yes
RollbackFailed	No	No	Yes	No	Yes
PreloadPaused	No	Yes	Yes	No	No
Preloading	No	No	No	No	No
PreloadFailed	No	No	No	No	Yes

Troubleshooting and Logs

This section provides a summary of modifications tables and logs for work order administration.

Modifications Tables

There are three seperate tables for tracking different types of modifications for a work order. It is important to familiarize yourself with these tables before executing a work order, as these views can be helpful in troubleshooting issues.

Local Configuration View

The local configuration view (LCV) is only available for global parameter changes and provides a list of top-level element changes made by the user for the selected global configuration. If you create a SIP manipulation header rule, the header rule will not appear in this table. The Type column lists the top-element; sip-manipulation in this instance.

Please consult Viewing Modifications in the LCV for instructions to access the LCV.

Device Tasks Table

The Device tasks table is located beneath the Work orders table. When you select a work order in the table, the Device tasks table populates with a list of operations for the targeted devices in your work order.

You can select a device task and click **Preview** for more information.

Please consult Device Tasks Table for more information on device tasks.

Preview Screen

You access the Preview Screen through the Device tasks table. You select a work order, and then a device task. Click **Preview** to obtain a detailed view of modifications for this device. The Preview screen provides a summary of changes made by the user and the changes necessary for that targeted device due to the configuration differences between a global configuration and a targeted device's configuration.

For example, if you add a third-level sub-element to a global configuration, it is possible that one of your targeted devices did not contain the higher-level elements in their current saved configuration. Those top-level instances are added by the Oracle Communications Session Element Manager server, and the Preview screen for that device logs these required updates. A Preview screen can differ for every targeted device in a work order based on their original configurations.

The Preview screen contains two tables: Attribute parameters modifications and Elements addition/deletion tables. Please consult Viewing Attribute Parameters Modification and Elements Addition Deletion Tables for instructions to access the Preview screen tables.

Logs

You can view logs for work orders and device tasks when a work order is running, or after it has been executed. Some of the items included in a log are:

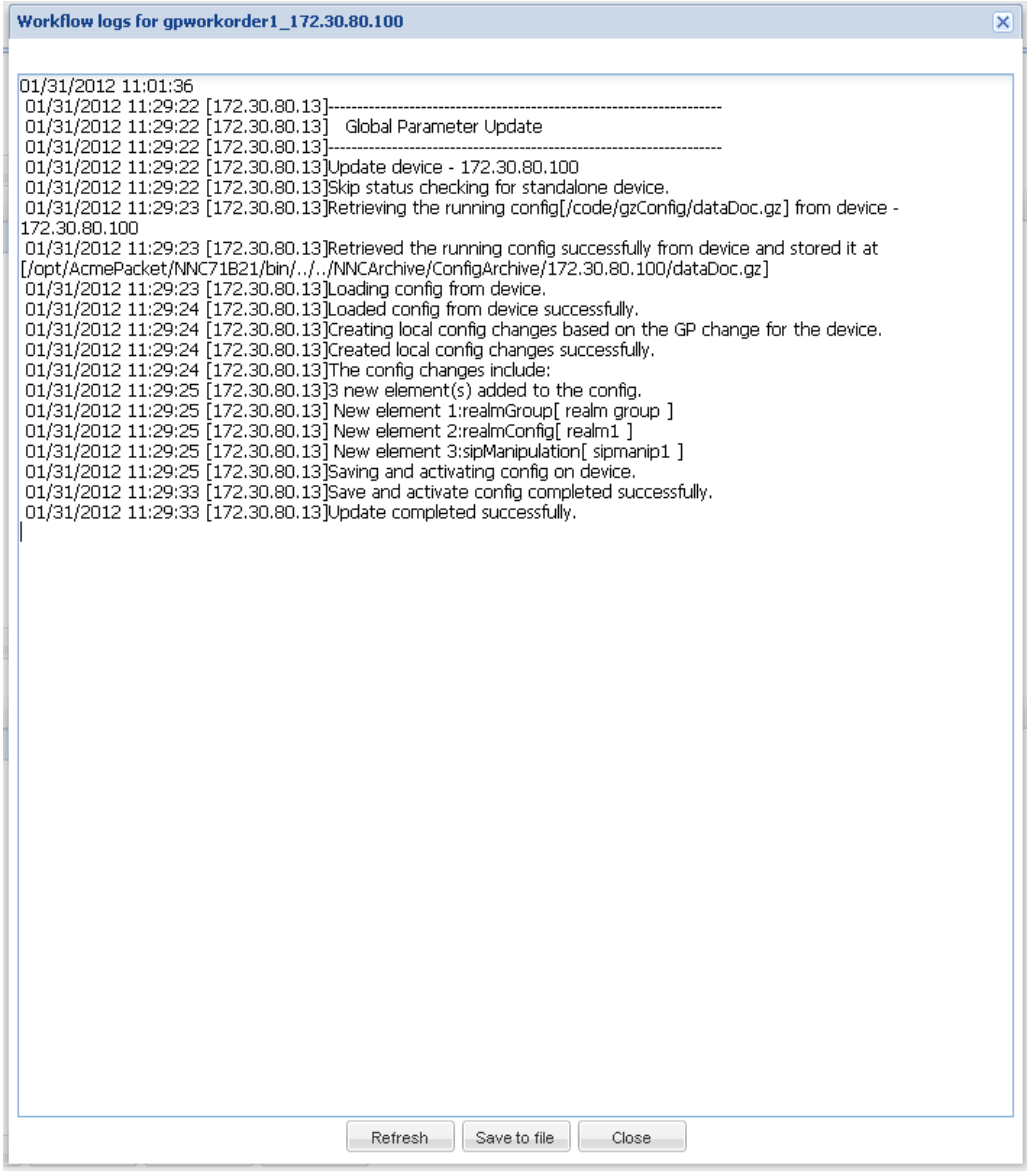
- Global parameter changes, including addition, modification, and deletion.
- Software archive and software upgrade.
- Work order actions, including pause, start/resume, abort/rollback, and commit.
- Work order task actions, including pause, resume, abort/rollback, and resubmit.

Work Order Logs

In the Work orders table, you can select a work order and click **Logs**. Work order-level messages pertain to the actions and state of the work order itself. You can view lower-level device tasks in the device tasks logs. Below is an example of a work order log.

Device Tasks Logs

In the Device tasks table of any work order, you can select a device task and click **Logs**. These logs provide a device task-level of logging messages. Below is an example of a device task log. You can see the steps required for adding configuration.



Audit Trail Log

The following information is included in the audit trail log.

1. Work order actions such as Pause, Start, Resume, Abort, Rollback and Commit.
2. Work order actions for tasks such as Pause, Resume, Abort, Rollback and Resubmit.
3. Global parameter changes.
4. Global configuration creation, modification and deletion.
5. Software image addition and deletion to the software image archive.