Oracle® Communications Session Delivery Manager

Element Manager
Release 7.4
Formerly Net-Net Central

May 2014

Notices

Contents

About this Guide

The Oracle Communications Session Delivery Manager Element Manager Guide contains an overview of the Session Element Manager graphical user interface (GUI), and describes device management.

Related Oracle Communications Session Delivery Manager Documentation

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

Document Name	Document Description
Release Notes	Contains information about the administration and software configuration of the Oracle Communications Session Delivery Manager feature support new to this release.
Installation Guide	Contains graphical and next mode installation information.
High Availability Guide	Describes Oracle Communications Session Delivery Manager High Availability (HA) and the HA cluster, which is a network of tightly-linked servers. HA provides continuous management of the SDM system.
Web Services SOAP XML Provisioning API Guide	Provides a full description of the individual interface definitions that make up the Application Programming Interface (API).
Core Functionality Guide	Contains an overview of the Oracle Communications Session Delivery Manager graphical user interface (GUI), detailed information about managing devices in Net-Net Central, and Net-Net Central licenses.
Session Element Manager Guide	Contains detailed information pertaining to the Session Element Manager application and describes the dashboard summary view, audit log, fault, and performance views.
Session Route Manager Guide	Contains detailed information about centrally automating the management and distribution of routing data.
Quick Start Guide	Contains a brief description of the GUI, along with information on how to add a device and perform basic configuration tasks.
Administration Guide	Contains information about security administration, which lets you create new users and new user groups, and set group-based authorization.
Report Manager Installation Guide	Contains instructions for installing Report Manager's dependencies and registering BI Publisher.
Report Manager User Guide	Contains information about configuring collection groups and creating reports.

Revision History

Date	Description
May 2014	• Initial release

1

Getting Started

Overview

Element Manager enhances the core system by providing provisioning capabilities, along with fault and performance statistics for your managed devices. The sliders included with Element Manager are:

- Dashboard Manager: Provides a dashboard summary view with at-a-glance device status and key performance indicators for your managed devices
- Configuration Manager: Load and provision devices:
  - Customize your configuration by choosing from three distinct configuration view styles. Top-level elements are grouped by:

    Default: Displayed logically, according to the type of configuration required

    ACLI: Displayed as they would appear in the ACLI: by media-manager, session-router, system, or security

    List: Displayed in an alphabetically-ordered list
  - Conduct view-to-view navigation: Switch from one configuration view to another configuration view, with the content area automatically refreshing to the last attribute displayed from the previous view
  - View your own modifications made to a device via a local configuration view, which details your configuration changes
- Fault Manager: View events, alarms, and trap summary data
- Performance Manager: View performance statistics collected from the Net-Net SBC, such as system, SNMP, IP, environmental, and so on

About Managed Devices

Oracle Communications Session Delivery Manager’s Element Manager application allows for the loading, configuring, and managing of devices, (Net-Net SBC). This release of Oracle Communications Session Delivery Manager can manage the following devices:

- C-Series—Also known as the Net-Net 4000 series and Net-Net 3000 series. The Net-Net 4000 series contains two systems: the Net-Net 4250 and Net-Net 4500. The Net-Net 3000 series contains two systems: the Net-Net 3800 (Sku 3810) and Net-Net 3820.
- D-Series—Also known as the Net-Net 9000 series, it contains one system: the Net-Net 9200.
- E-Series—Also known as the Net-Net 2000 series, it contains one system: the Net-Net 2600.

Minimum Net-Net SBC Configuration

The Net-Net SBC configurations you plan to manage using Oracle Communications Session Delivery Manager must have the following information configured in order to be properly loaded into Configuration Manager. To verify the minimum configuration for Net-Net SBCs you plan to manage, see the following documentation:

- Oracle Communications Session Delivery Manager Configuration Guide for details about configuring a Net-Net SBC using the Acme Command Line Interface (ACLI)
- Net-Net ACLI Reference Guide to refer to all ACLI commands

Boot Parameters

Boot parameters specify the information your Net-Net SBC system uses at boot time when it prepares to run applications. The Net-Net SBC system's boot parameters include the Net-Net SBC system's IP address for the management interface (wancom0) and the target name.

Oracle Communications Session Delivery Manager uses the target name to uniquely identify a Net-Net SBC from among the list of Net-Net SBCs in the content area. You need to ensure that all Net-Net SBCs you plan to manage, thus load, with Oracle Communications Session Delivery Manager have unique target names. Otherwise, a list of Net-Net SBCs, all with the default name acmesystem would appear in the list.

Ensure the following boot parameters have been configured:

- wancom0 IP address and mask
- target name is set to a unique name (do not use the default name acmesystem)

System Configuration Element

You need to ensure the system-config element has been configured. This element establishes general system information and settings, for example:

- Contact information for this Net-Net SBC system for SNMP purposes
- Identification of the Net-Net SBC system for SNMP purposes
- Physical location of the Net-Net SBC system for SNMP purposes
- Whether SNMP is enabled on the system
- Whether traps are enabled
- Default gateway

For complete details about system configuration, see the Net-Net 4000 Configuration Guide and the Net-Net ACLI Reference Guide.

SNMP Community Element

You need to ensure the snmp-community element is configured. This element defines the Oracle Communications Session Delivery Manager server from which the Net-Net SBC system will accept SNMP requests. Specifically, you need to ensure:

- IP address list contains the address of the host upon which Oracle Communications Session Delivery Manager server is running. IP address(es) for SNMP communities for authentication purposes.
- Access mode is read-only

Note: If configuring the snmp-community element for a cluster, you must add both server IP addresses in the cluster.

If you change the snmp-community values for your Net-Net SBC, you must remove the SBC from the Device Manager, and then add it again for the Oracle Communications Session Delivery Manager server to update this SNMP information.

Trap Receiver Element

You need to ensure the trap-receiver element is configured. This element defines the Oracle Communications Session Delivery Manager server to which the Net-Net SBC system sends SNMP traps for event reporting. Specifically, you need to ensure:

- IP address is that of the Oracle Communications Session Delivery Manager server
- Filter level is set to All
- Community name matches the name in the SNMP community element

Note: If configuring the trap-receiver element for a cluster, you must add both server IP addresses in the cluster.

Accessing Session Delivery Manager

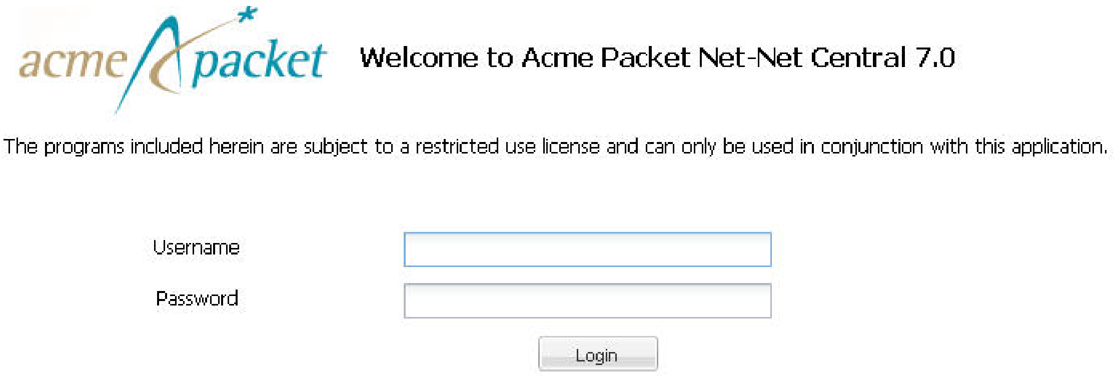
You can access the Oracle Communications Session Delivery Manager server by using two address formats (as shown in step 2.)

To access Oracle Communications Session Delivery Manager:

1. Open a Web browser.
2. Connect to the Oracle Communications Session Delivery Manager server using one of the following address formats:

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

The Login screen appears.

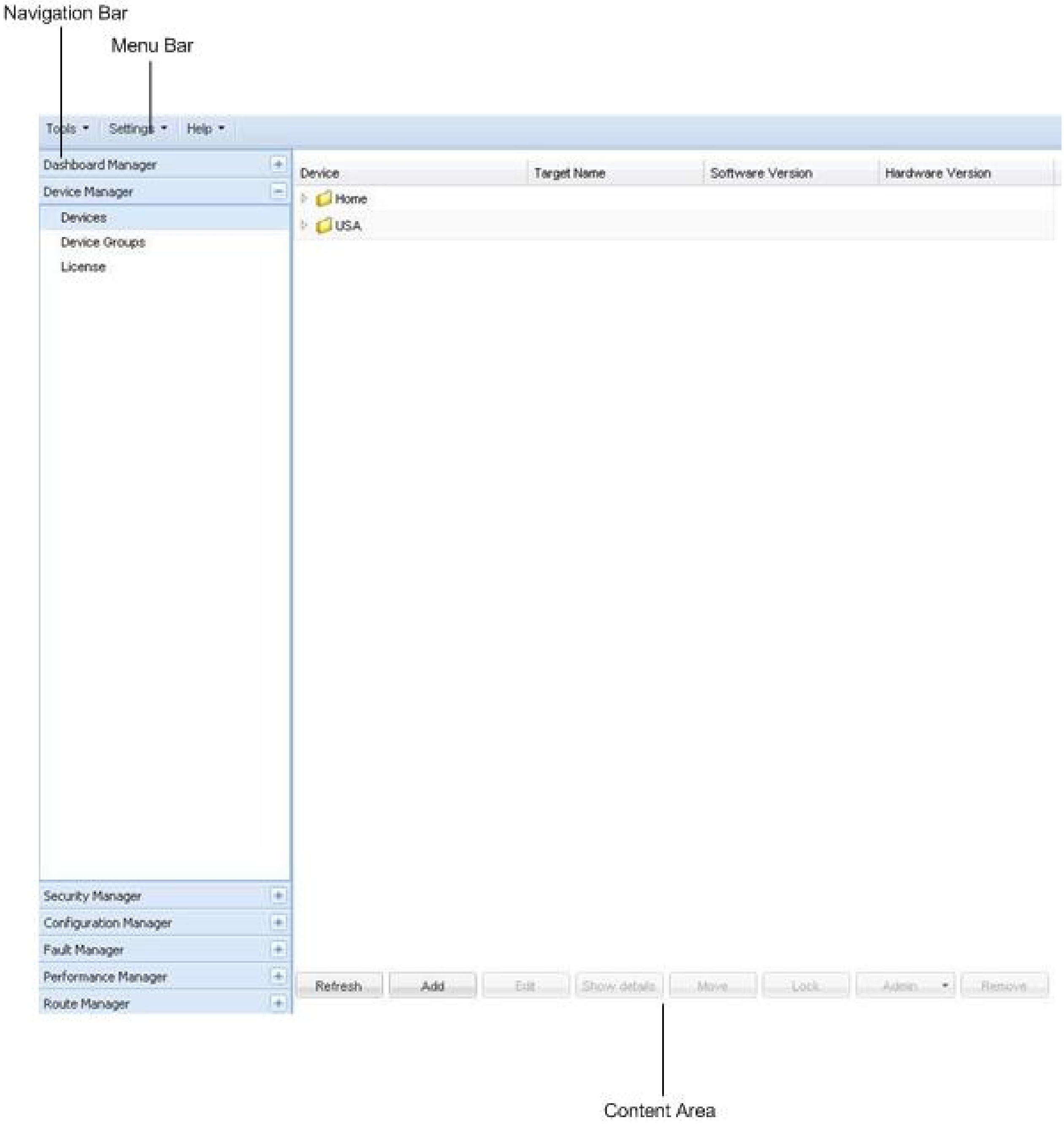


Welcome to Acme Packet Net-Net Central 7.0

The programs included herein are subject to a restricted use license and can only be used in conjunction with this application.

3. Enter your user name and password and click Login. (The default username is admin, with a default password of admin.)

You have now accessed Oracle Communications Session Delivery Manager.



Note: When you login to Oracle Communications Session Delivery Manager, your display will differ based on your licensed applications.

2

Using Element Manager

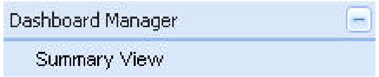
Introduction

Net-Net Cetnral’s Element Manager lets you configure and manage your devices and view fault and performance data.

The following sections describe the sliders included with Element Manager.

Dashboard Manager

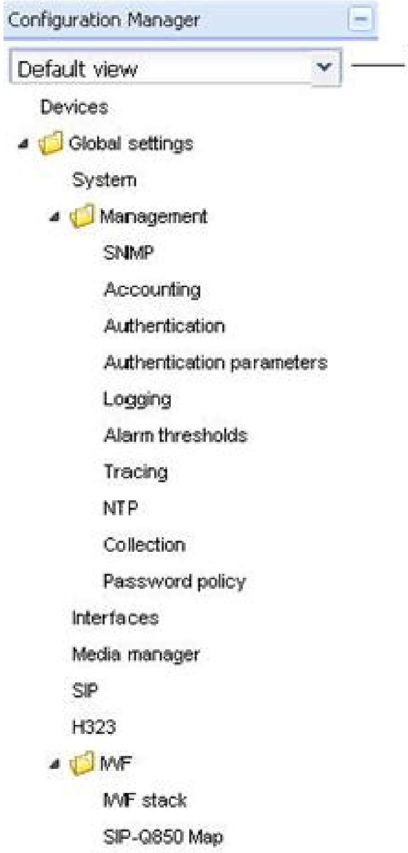
Dashboard Manager contains the summary view where you view a dashboard summary of critical alarm counts, health scores, CPU usage statistics, and other data for your devices.



For more information about these statistics, see the Summary View chapter of this guide.

Configuration Manager

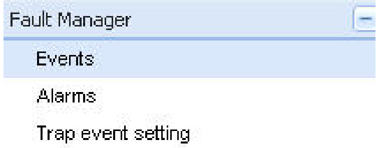
Configuration Manager lets you load and configure your devices. Once you finish making your configuration changes, you apply them and perform an update to save the changes to the Net-Net SBC.



This is a partial listing of this slider.

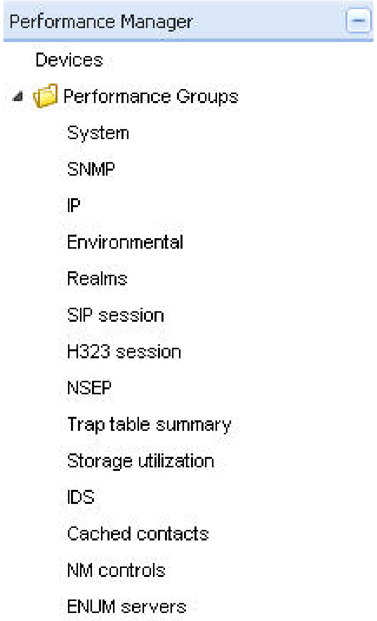
Fault Manager

Fault Manager contains information pertaining to events (caused by actions that generate alarms, entries in a log file, or SNMP traps), alarms, and trap event settings for your devices. You can monitor events, alarms, or trap data and save the data to a file. You also clear alarms within Fault Manager.



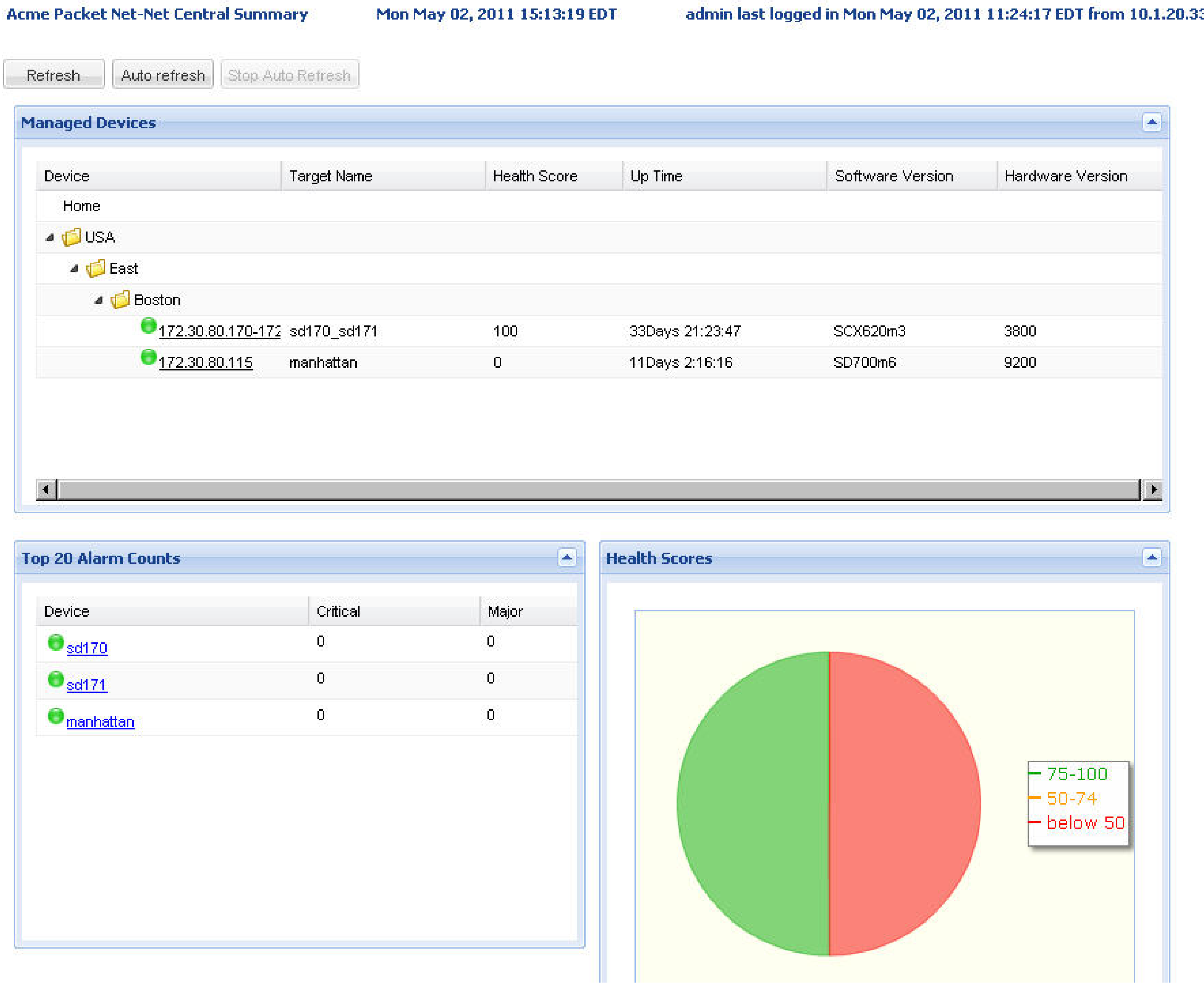
Performance Manager

Performance Manager displays real-time, on-demand performance statistics for monitoring performance and utilization. You can view this data or save it to a file.



Content Area

The content area is your work area. You can also view fault and real-time performance data in the content area. The information that appears depends on which navigation slider you select. The information that appears depends on which navigation slider you select. The following example shows Dashboard Manager, summary view, which appears with Element Manager.



Acme Packet Net-Net Central Summary Mon May 02, 2011 15:13:19 EDT admin last logged in Mon May 02, 2011 11:24:17 EDT from 10.1.20.33

Managed Devices

Device	Target Name	Health Score	Up Time	Software Version	Hardware Version
Home					
USA					
East					
Boston					
● 172.30.80.170-172	sd170_sd171	100	33Days 21:23:47	SCX620m3	3800
● 172.30.80.115	manhattan	0	11Days 2:16:16	SD700m6	9200

Top 20 Alarm Counts

Device	Critical	Major
● sd170	0	0
● sd171	0	0
● manhattan	0	0

Health Scores

Working with Configuration Views

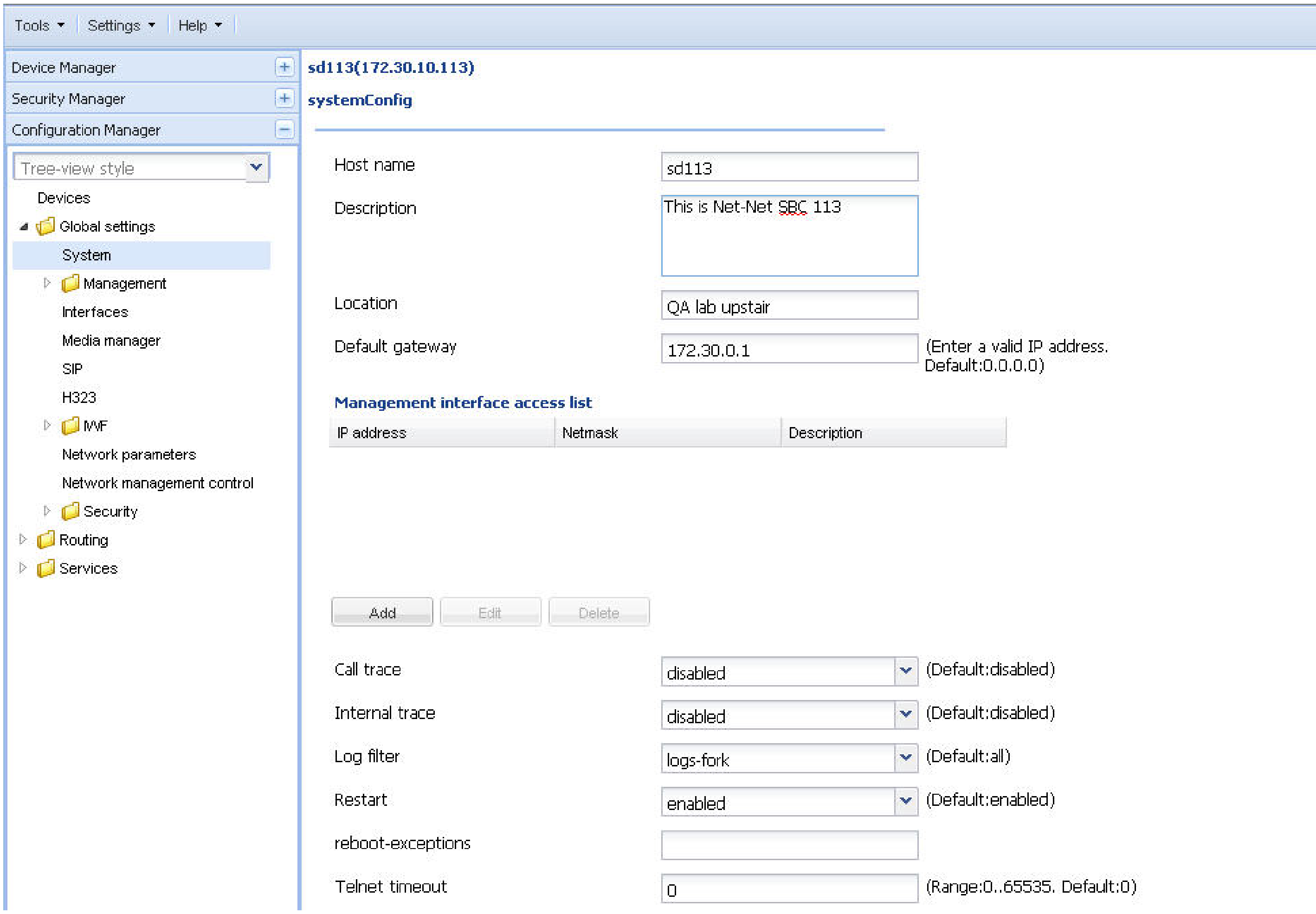
There are three configuration views within Configuration Manager: Default, ACLI, and List. These views let you navigate around the top-level configuration elements in a specific way. The following sections describe each of these views.

No matter which view you select, you will be able to peruse all of the possible top-level configuration elements for your device. Once you select your view, and configuration element, the content area will display all attributes (or parameters) associated with this configuration element.

Navigating Between Configuration Views

You can switch between views at any time during your session. When you switch from one view to another view, the content area automatically opens to the top-level element you were working in 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 content area will open to the top-level element, media-manager.

Below is an example of the Default view with the top-level element, System, selected. The content area displays all attributes for the system element.



sd113(172.30.10.113)

systemConfig

Host name	sd113	
Description	This is Net-Net SBC 113	
Location	QA lab upstair	
Default gateway	172.30.0.1	(Enter a valid IP address. Default:0.0.0.0)

Management interface access list

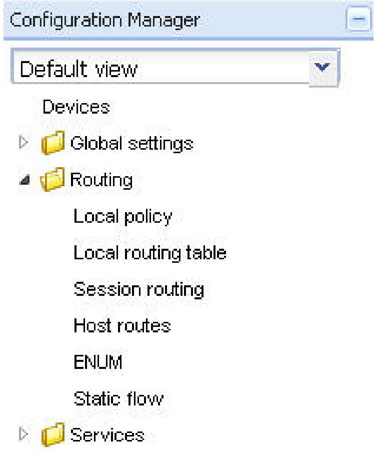
IP address	Netmask	Description

Call trace	disabled	(Default:disabled)
Internal trace	disabled	(Default:disabled)
Log filter	logs-fork	(Default:all)
Restart	enabled	(Default:enabled)
reboot-exceptions		
Telnet timeout	0	(Range:0..65535. Default:0)

Using the Default View

As the name implies, this is the first view presented, by default. With the default view, the top-level configuration elements are grouped logically, according to the type of configuration required: managing global settings and security, configuring routing, and defining services (media, signaling, and agents.) All top-level elements, and their corresponding attributes (or parameters) are displayed using Oracle Communications Session Delivery Manager labels, and not using ACLI parameter names, for example, Proxy IP port, and not home-proxy-port.

In the Default view example below all top-level configuration elements related to routing, such as local policy, session routing, or ENUM are grouped together under Routing. You expand the configuration category folders (for example, Routing) to view the top-level elements for each category.



About Default View Groups

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.

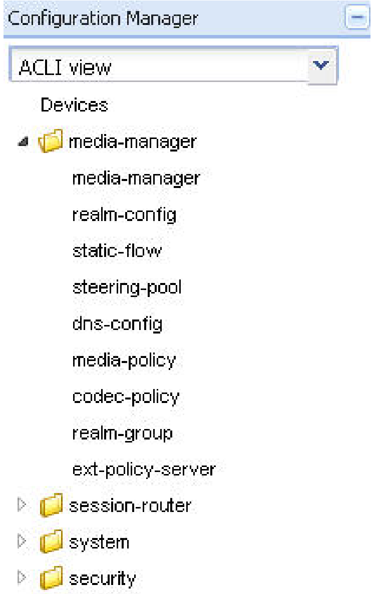
Configuration Categories	Sub-categories	Categories within Sub Categories
Global Settings	Management IWF Security	IKE
Routing		
Services	Media Signaling Agents	SIP, Translation, Call Admission Control

Using the ACLI View

With the ACLI view, the top-level elements are displayed as they would appear in the ACLI: grouped under media-manager, session-router, system, or security. All Oracle Communications Session Delivery Manager configuration labels are listed according to their corresponding ACLI parameter names (for example, home-proxy-port, and not Proxy IP port).

Note: Column width and table pagination persist throughout the session or until you resize the browser window.

The example below displays the top-level elements under media-manager.

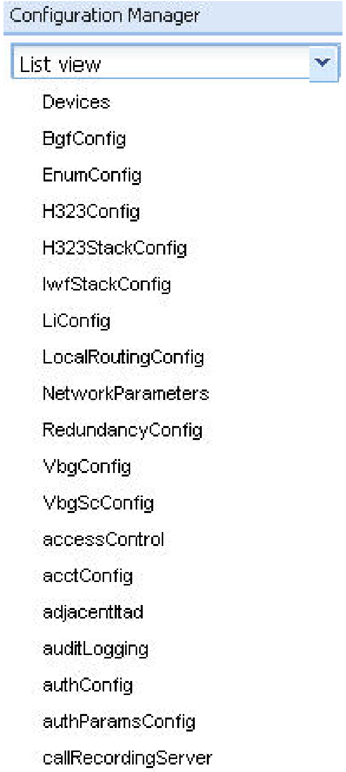


Using the List View

With the List view, the top-level elements are displayed in an alphabetically-ordered list, and in the ACLI parameter format, for example, enum-config and not ENUM. There is no special grouping as with the other two views.

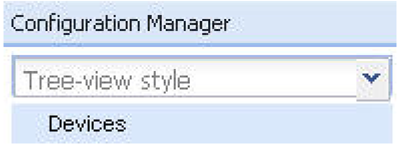
Note: Column width and table pagination persist throughout the session or until you resize the browser window.

This is an easy way to locate a top-level element if you are unsure of how it is grouped in the Default view or the ACLI view. For example:



About the Devices Element

The first category shown in Configuration Manager (for all three views) is Devices. When you click Devices, the content area displays the list of device groups and devices added to Oracle Communications Session Delivery Manager. From here, you select and load your device for configuration. In the example below, the Default view is selected, with Devices displayed along with the devices listed in the Boston device group. For more information about loading a device for configuration, see *Loading a Configuration*.



About the Relationship with ACLI

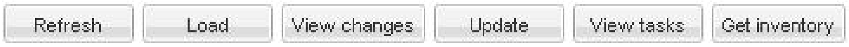
Oracle Communications Session Delivery Manager provides a a GUI-based approach to managing Net-Net SBCs. It provides the ability to configure and monitor standalone Net-Net SBCs and clusters of servers, with configuration, fault, performance, and security management for the Oracle product line.

The ACLI is an administrative interface that communicates with other components of the Net-Net system. The ACLI is a single DOS-like, line-by-line entry interface that you can use to configure and monitor your Net-Net family of products.

You can use Oracle Communications Session Delivery Manager to perform almost all the same configuration and monitoring functions that can be performed using the ACLI. (See the Net-Net ACLI Reference Guide for more information about using the ACLI.) You can use both interfaces to work with Net-Net SBCs; even switching from Oracle Communications Session Delivery Manager to login to a Net-Net SBC and use the ACLI.

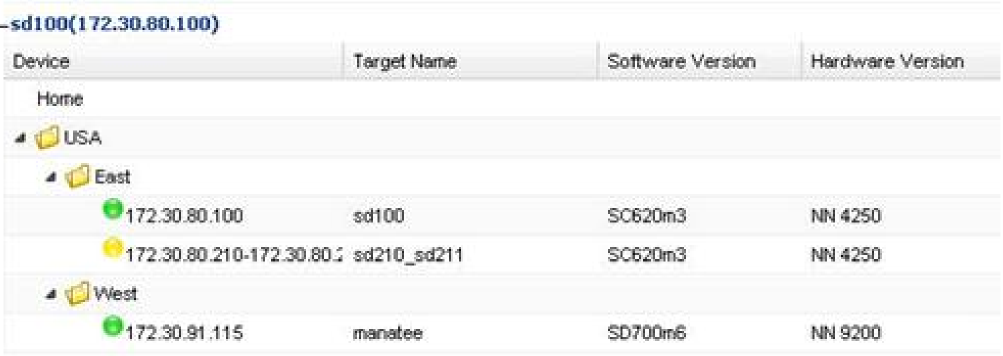
Performing Actions from Devices Display

At the bottom of the Device display there are six actions you can perform. When you invoke one of these actions, Oracle Communications Session Delivery Manager targets the last device loaded for editing, except for Refresh and Load. You must make sure the device you want to target is loaded.



The loaded device appears as header text above the Device table. In the example below, device sd100(172.30.80.100) is loaded for configuration changes.

This is the currently loaded managed device.



sd100(172.30.80.100)

Device	Target Name	Software Version	Hardware Version
Home			
USA			
East			
172.30.80.100	sd100	SC620m3	NN 4250
172.30.80.210-172.30.80.2	sd210_sd211	SC620m3	NN 4250
West			
172.30.91.115	manatee	SD700m6	NN 9200

The actions are explained in the table below.

Action	Description
Refresh	Refreshes all devices for all device groups listed. The Refresh button is always enabled
Load	The Load button is enabled after you select a device from the list of devices on the Devices display

Action	Description
	Once invoked, loads the configuration for the currently-selected device for editing. If a new configuration version is available, the corresponding device's configuration data is refreshed
View Changes	Displays a list of all configuration changes for the selected device. By default, the table initially displays the changes made by the current user. By changing the User parameter to another user, or to the value, all, you can view all users' changes in a single list. From View Changes, with the appropriate permissions assigned, you can: Refresh: Refreshes the data in the view changes list Undo Changes: Will undo all changes you made to this device. You cannot undo changes made by another user Change Owner: Allows you to transfer the ownership of your changes to another user. You cannot change the ownership of changes made by another user Update: Launches a dialog box with three options: Save and activate configuration (default), Save configuration, and Activate configuration. You cannot update the changes made by another user Save to file: Saves the data displayed to a text file in comma separated values (CSV) format
Update	Launches a dialog box with three options: Save and activate configuration (default): saves the configuration changes and activates the current configuration on the Net-Net SBC to make it the running configuration Save configuration: Saves the current configuration changes to the Net-Net SBC (targeted device) Activate configuration: Activates the current configuration on the Net-Net SBC to make it the running configuration
View tasks	View the device tasks (or operations) performed on this device
Get Inventory	Accesses configuration inventory details for this device

User Interaction

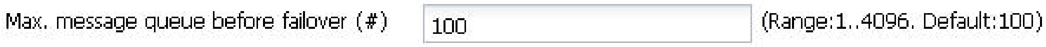
This section contains information about user-interaction scenarios, error messages, tool tips, configuration for single-instance elements, and configuration timestamps.

Methods

Oracle Communications Session Delivery Manager provides different methods for user interaction. Some examples of these methods are:

- Text fields
- Dialog boxes
- Combination boxes
- Checkboxes
- Options selector
- Radio buttons

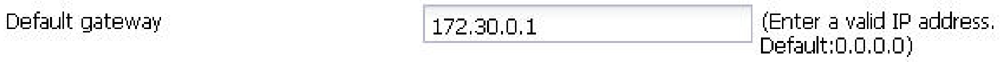
Often instructions are provided for a parameter. These instructions help you to understand the guidelines of your entry, whether or not this is a required field, and provides the default value, if there is one. For example:



Max. message queue before failover (#) 100 (Range:1..4096. Default:100)

Text Fields

Text fields allow you to manually enter information, usually with certain guidelines, for example, you can enter up to 25 characters, or you cannot include spaces in your entry. In the example below, there is a requirement to the right of the field to instruct you, which includes a default value for this parameter:



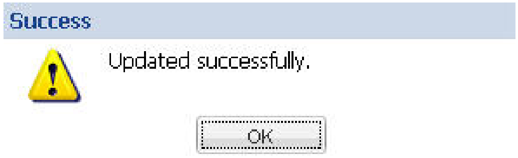
Default gateway 172.30.0.1 (Enter a valid IP address. Default:0.0.0.0)

Dialog Boxes

There are three types of dialog boxes most commonly found in Oracle Communications Session Delivery Manager:

- Alerts
- Informational
- Configuration-required

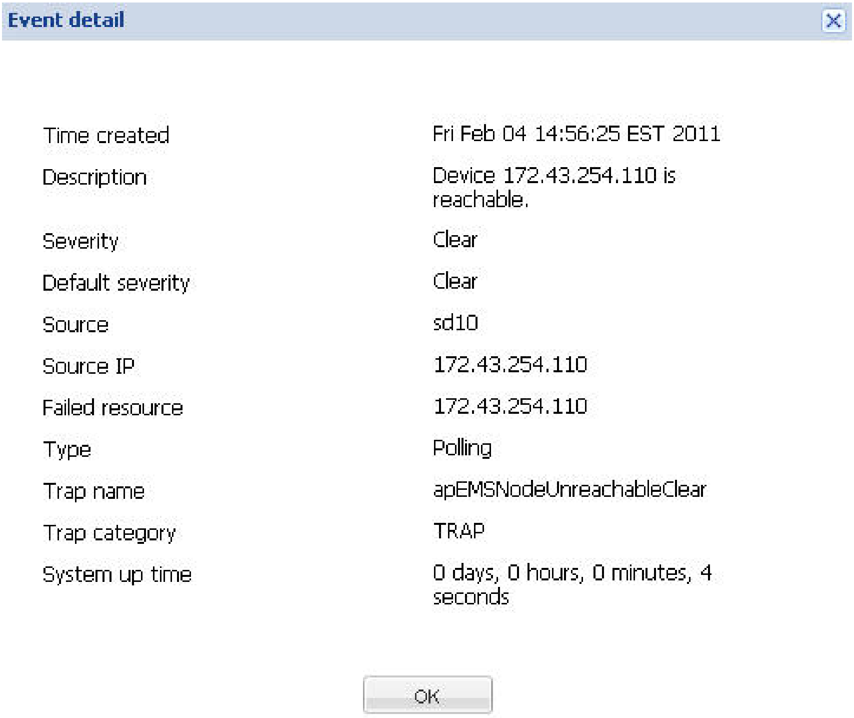
The simplest type of dialog box is an alert, which displays a message and can appear following an action, such as updating a parameter. This type of dialog box generally requires an acknowledgement, by clicking OK, to ensure the message has been read. For example,



Success

Updated successfully.

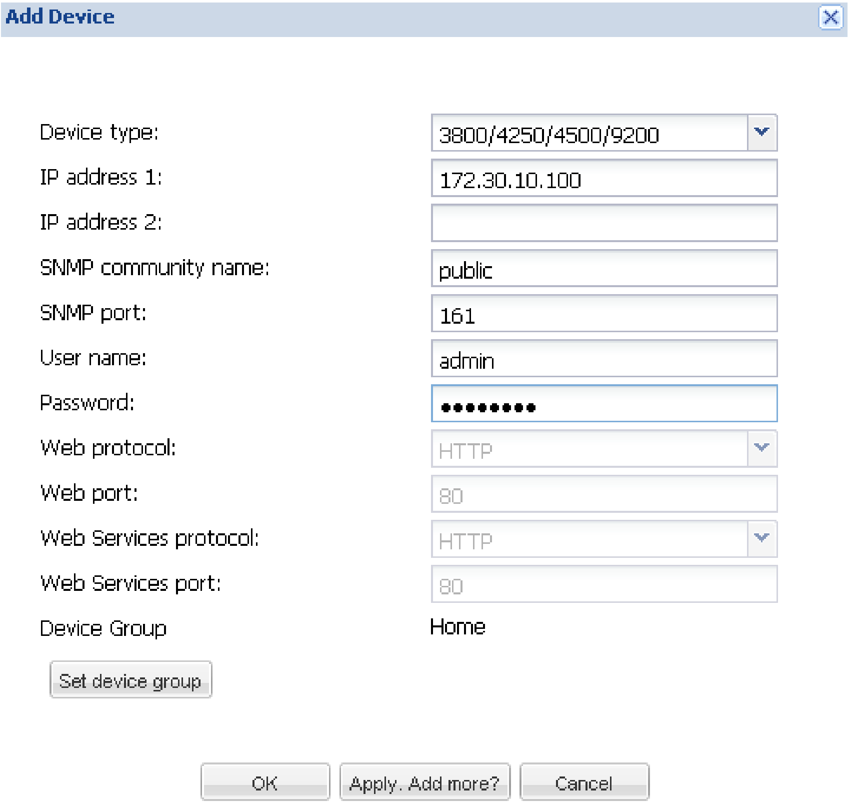
Dialog boxes can deliver additional information. For example, if you view an event in the Event table under Fault Manager and want more information, click the event to open a dialog box with more event detail. For example,



Event detail

Time created	Fri Feb 04 14:56:25 EST 2011
Description	Device 172.43.254.110 is reachable.
Severity	Clear
Default severity	Clear
Source	sd10
Source IP	172.43.254.110
Failed resource	172.43.254.110
Type	Polling
Trap name	apEMSNodeUnreachableClear
Trap category	TRAP
System up time	0 days, 0 hours, 0 minutes, 4 seconds

Dialog boxes can also be a means to group parameters together, for example, all parameters required for adding a device. Typically, you open this type of dialog box by clicking a button, such as Add or Edit. You can encounter different user-input methods within a dialog box. For example:

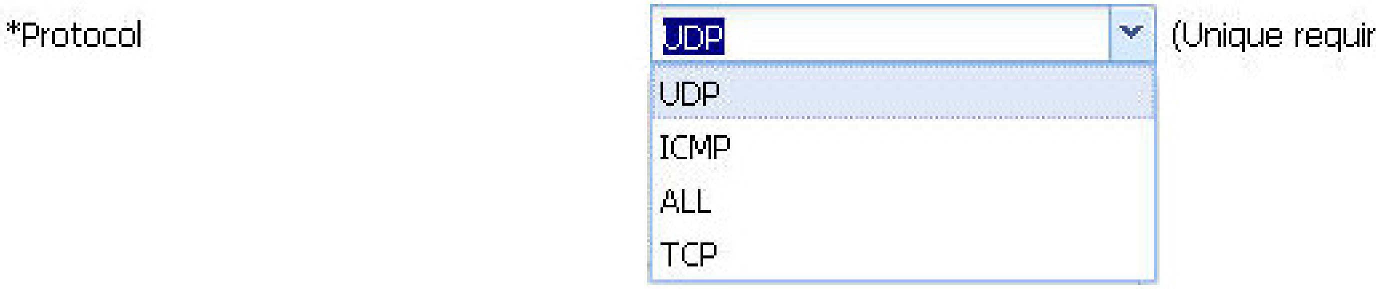


Add Device

Device type:	3800/4250/4500/9200
IP address 1:	172.30.10.100
IP address 2:	
SNMP community name:	public
SNMP port:	161
User name:	admin
Password:	●●●●●●●●●
Web protocol:	HTTP
Web port:	80
Web Services protocol:	HTTP
Web Services port:	80
Device Group	Home

Combination Boxes

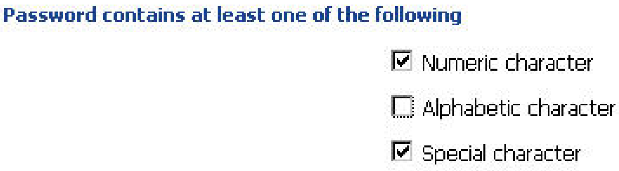
With combination boxes, you expand a pre-defined list of choices by clicking on an arrow to the right of the text field. To make your selection, you click your choice in the list. For example:



*Protocol: UDP (Unique requir

Checkboxes

With checkboxes, you can select one or more choices from a pre-defined list of choices list by clicking in the box to check it, for example:



Password contains at least one of the following

☑ Numeric character

☐ Alphabetic character

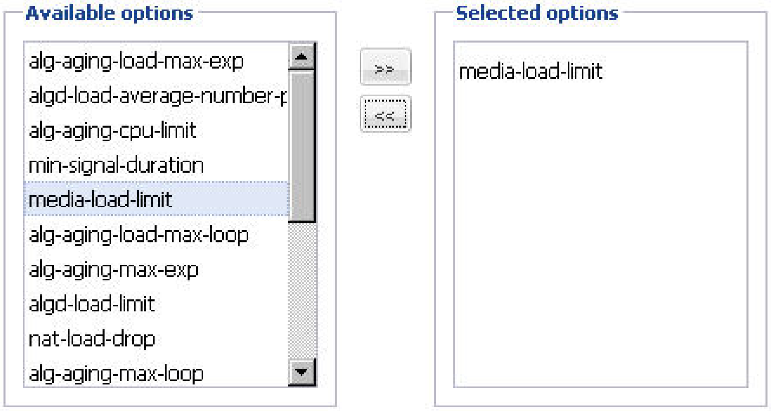
☑ Special character

Options Selector

When configuring options for certain Net-Net SBC features, you click the option in the Available options list to select it, and you click >> to move it into the Selected options list. You repeat this process to add additional options.

To remove an option from the Selected options list, you click the option in the Selected options list to select it, and you click << to move the option back into the Available options list.

Below is an example of media-load-limit moved into the Selected options list:



Available options:

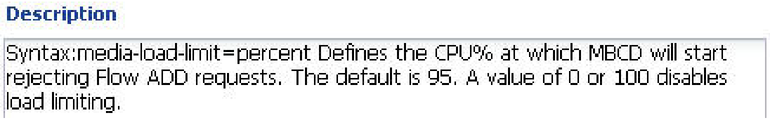
- alg-aging-load-max-exp
- algd-load-average-number-p
- alg-aging-cpu-limit
- min-signal-duration
- media-load-limit
- alg-aging-load-max-loop
- alg-aging-max-exp
- algd-load-limit
- nat-load-drop
- alg-aging-max-loop

Selected options:

- media-load-limit

User-Defined Options

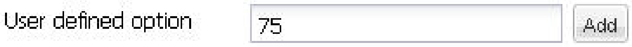
Some options require additional configuration, for example, adding a percentage. In such cases, an options description provides you with guidelines for your entry. For example, the description for media-load-limit is:



Description

Syntax:media-load-limit=percent Defines the CPU% at which MBCD will start rejecting Flow ADD requests. The default is 95. A value of 0 or 100 disables load limiting.

You enter text into the User defined option text field and click Add to update the option with your entry, for example:

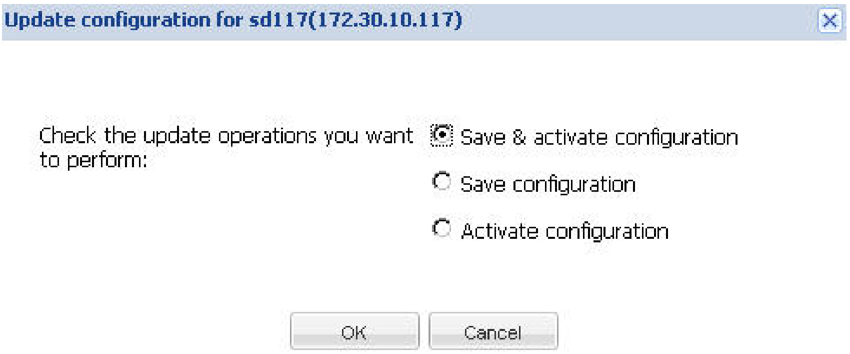


User defined option: 75

To edit a user-defined option, click Edit at the bottom of the Options selector dialog box.

Radio Buttons

With radio buttons, you select one choice only from a pre-defined list of choices. You click the radio button next to your choice to make your selection. For example:



Update configuration for sd117(172.30.10.117)

Check the update operations you want to perform:

● Save & activate configuration

○ Save configuration

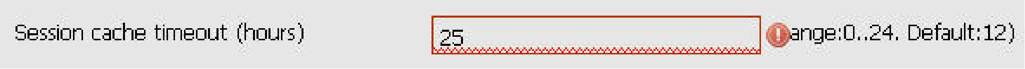
○ Activate configuration

Error Messages

If you incorrectly enter a value in a text field, and try to apply this change, you will receive an error message, along with an error panel detailing your input error. For example, if you enter a value beyond the valid value range, you will receive a validation error.

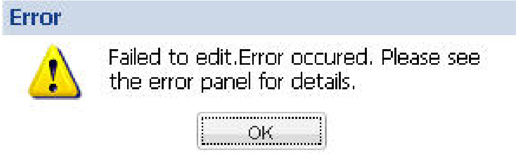
Entering an Incorrect Value

In the example below, an incorrect value was entered. Subsequently, the text field is outlined in red, with an exclamation point, letting you know there was an error:



Session cache timeout (hours) 25 ange:0..24, Default:12)

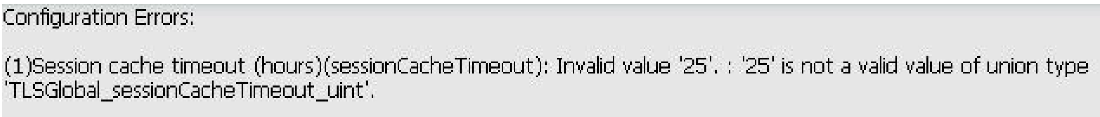
An error message pops up in the content area directing you to an error panel with a description of your mistake, as shown in the example below. You must click OK to clear this error message.



Error

Failed to edit.Error occured. Please see the error panel for details.

The error panel is shown in the top-left corner of the content area. Below is the example of the error panel, Configuration Errors, associated with the Session cache timeout (hours) mistake referenced above:

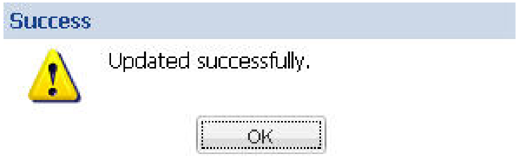


Configuration Errors:

(1)Session cache timeout (hours)(sessionCacheTimeout): Invalid value '25'. : '25' is not a valid value of union type 'TLSGlobal_sessionCacheTimeout_uint'.

Reentering a Correct Value

Once you click OK to clear the error message, you can reenter a correct value in the text field. You must click Apply to apply your value. When correct, you will receive a success message. Click OK to clear the message.

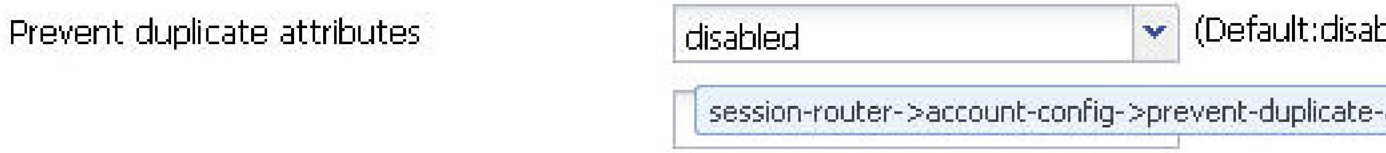


Success

Updated successfully.

Using Tool Tips

When configuring your device in Configuration Manager, position your cursor over a parameter field or checkbox to view a tool tip. Tool tips display the complete path to, and name of, the corresponding ACLI parameter. For example,



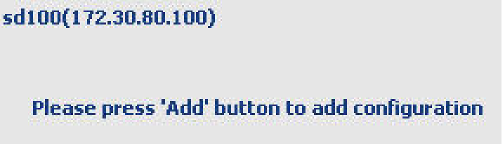
Prevent duplicate attributes disabled (Default:disab

session-router->account-config->prevent-duplicate-

Note: Tool tips will display no matter which view you use in Configuration Manager: Default, ACLI, or List view.

Configuring Single-Instance Configuration Elements

With multi-instance elements, the configuration parameters load automatically in the content area once you select your top-level element. When configuring single-instance configuration elements, such as accounting or session routing, you will be prompted to add the configuration to the content area by clicking Add. For example:.



sd100(172.30.80.100)

Please press 'Add' button to add configuration

Once you click Add at the bottom of the content area, the accounting parameters load and a success message appears.

You must click OK to clear the message to begin configuring.

Configuration Timestamp

You might see a configuration timestamp while configuring parameters. This timestamp is found in the content area, for example:

Last modified by	NNC_admin_172.43.0.105
Last modified date	2011-02-17 16:25:03

The configuration timestamp displays last modified information for configuration changes made.

When you make configuration changes to elements, the Last modified by field displays the following information:

Last modified by:

- Oracle Communications Session Delivery Manager identifier
- Name of the user that made the modification
- IP address of the host machine running Oracle Communications Session Delivery Manager

Last modified date:

- Date and time, which is displayed in the string date/time format, YYYY-MM-DD HH:MM:SS, for example 2011-02-17 16:25:03

Note: If a sub-element is modified, the timestamp belonging to the element is updated to indicate the modification time.

Loading a Configuration

You load a device's configuration by retrieving the device's configuration from the Net-Net SBC and loading it into the Oracle Communications Session Delivery Manager database. To do this, you target the specific device you want to load from the Configuration Manger device table. This process is called loading a local configuration copy. It is an on-demand process, whereby you do not have to replicate large device configurations and retains the Net-Net SBC as the master database.

You must first associate the devices you add in Device Manager before you can load your device configurations. For more information about adding devices, see Oracle Communications Session Delivery Manager Core Functionality Guide, Managing Devices.

Associating Devices

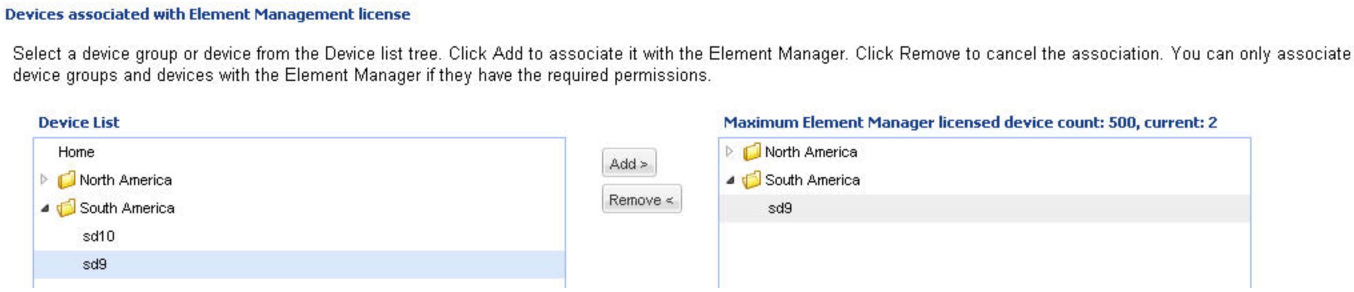
When you associate a device you link it to your Element Manager license. Your license allows you to configure a set number of devices at one time.

For more information about licensing, see the Oracle Communications Session Delivery Manager Core Functionality Guide, Viewing Oracle Communications Session Delivery Manager License Information.

You can associate one device at-a-time, or you can associate all devices within a device group, if your license permits.

To associate a device to the Element Manager License:

1. Expand the Configuration Manager slider.
2. Click Devices. The Device table appears in the content area.
3. Click Add devices. The Devices associated with Element Manager license appears in the content area.
4. From the Device list, expand your device group folder and click the device you want to associate.
5. Click Add > to move your device to the Maximum Element Manager licensed device count table.



Devices associated with Element Management license

Select a device group or device from the Device list tree. Click Add to associate it with the Element Manager. Click Remove to cancel the association. You can only associate device groups and devices with the Element Manager if they have the required permissions.

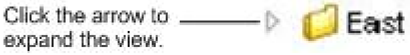
6. Click OK. A success dialog box appears.
7. Click OK.

Your device is associated with your Element Manager license so you can load your device configuration.

Loading a Local Configuration Copy

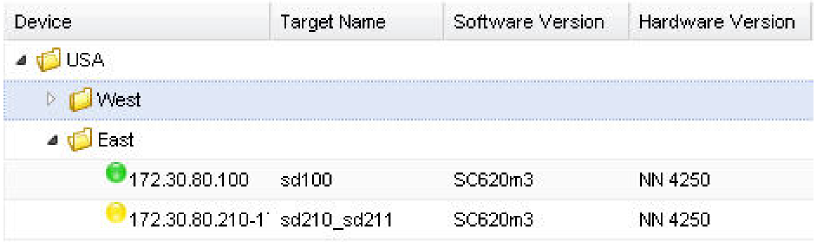
To load a local configuration copy of your device for configuration:

1. Expand the Configuration Manager slider.
2. Click Devices. The Device table appears in the content area.
3. Click the arrow next to the device group folder to expand the list of devices within this device group.



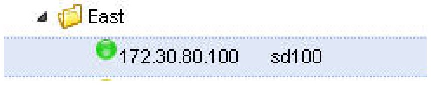
Click the arrow to expand the view.

The list of devices appears for this device group.

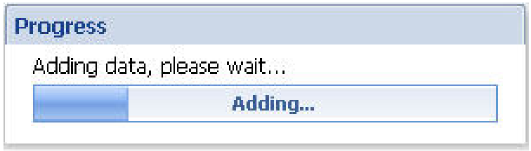


Device	Target Name	Software Version	Hardware Version
USA			
West			
East			
172.30.80.100	sd100	SC620m3	NN 4250
172.30.80.210-1'	sd210_sd211	SC620m3	NN 4250

4. Click the device you want to load and click Load.



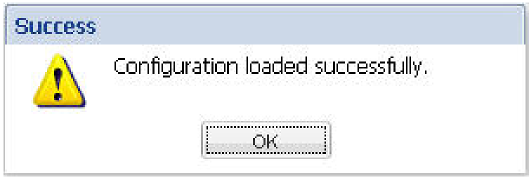
A Progress dialog box appears.



Progress

Adding data, please wait...

5. A Success dialog box appears. Click OK.

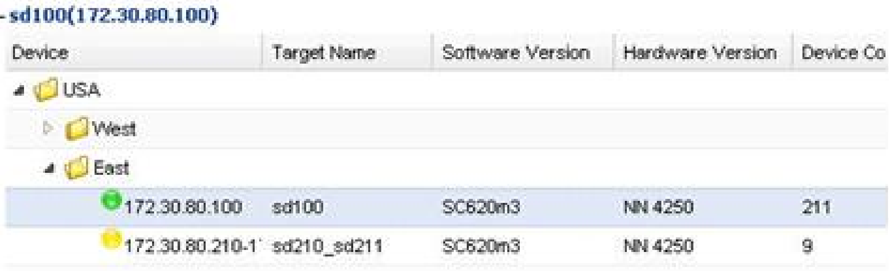


Success

Configuration loaded successfully.

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

This is your loaded device.



sd100(172.30.80.100)

Device	Target Name	Software Version	Hardware Version	Device Co
USA				
West				
East				
172.30.80.100	sd100	SC620m3	NN 4250	211
172.30.80.210-1	sd210_sd211	SC620m3	NN 4250	9

Configuration Schema Upload

You can upload a configuration schema into Net-Net Central by selecting and uploading a configuration file. Net-Net Central validates the schema to ensure it is a proper .XSD file. The uploaded schema is replicated to all members within a cluster.

Automatic XSD Loading

Net-Net Central automatically attempts to load the XSD of a C-Series device in the event the release was not provided with your version of Net-Net Central. New configuration elements can be configured from the List and ACLI view in the even that your SBC version is not supported a Net-Net Central release.

The XSD will be loaded during the following procedures:

- Adding a Device
- Loading a Configuration
- Updating SBC Software (via the NNC GUI)

Upload a Configuration Schema

1. Select the Tools menu and click Upload configuration file.
2. Click Browse... to navigate to a valid .xsd file.
   A file browsing dialog appears.
3. Select the configuration schema you want to upload and click Open.
4. Click Upload to start the upload process.
   A dialog appears with a success or error message.

After your Configuration is Loaded

Once your device's configuration copy is loaded, there are actions you can perform in Configuration Manger under Devices.

Performing Actions with Loaded Configurations

The actions are explained in the table below.

Action	Description
Refresh	Refreshes all devices for all device groups listed. The Refresh button is always enabled
Load	The Load button is enabled after you select a device from the list of devices on the Devices display Once invoked, loads the configuration for the currently-selected device for editing. If a new configuration version is available, the corresponding device's configuration data is refreshed
View Changes	Displays a list of all configuration changes for the selected device. By default, the table initially displays the changes made by the current user. By changing the User parameter to another user, or to the value, all, you can view all users' changes in a single list. From View Changes, with the appropriate permissions assigned, you can: Refresh: Refreshes the data in the view changes list Undo Changes: Will undo all changes you made to this device. You cannot undo changes made by another user Change Owner: Allows you to transfer the ownership of your changes to another user. if you have admin privileges. You cannot change the ownership of changes made by another user Update: Launches a dialog box with three options: Save and activate configuration (default), Save configuration, and Activate configuration. You cannot update the changes made by another user Save to file: Saves the data displayed to a text file in comma separated values (CSV) format
Update	Launches a dialog box with three options: Save and activate configuration (default): saves the configuration changes and activates the current configuration on the Net-Net SBC to make it the running configuration Save configuration: Saves the current configuration changes to the Net-Net SBC (targeted device)Activate configuration: Activates the current configuration on the Net-Net SBC to make it the running configuration Activate configuration: Activates the current save configuration on the Net-Net SBC to make it the running configuration The first two options are only available if there 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	View the device tasks (or operations) performed on this device
Get Inventory	Accesses configuration inventory details for this device

Configuration Element Search

The Configuration Element Search allows you to search and filter the instances within an element type's paged table.

Attributes that make up the column headings of the table become available as input filters for the search. Column headings that summarize subelements such as Session agent group -> Session agents and from -> addr are not included in the search results.

For example:

Results in the following search filters:

Filter Search Criteria

The search filters you enter must follow these guidelines:

- 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

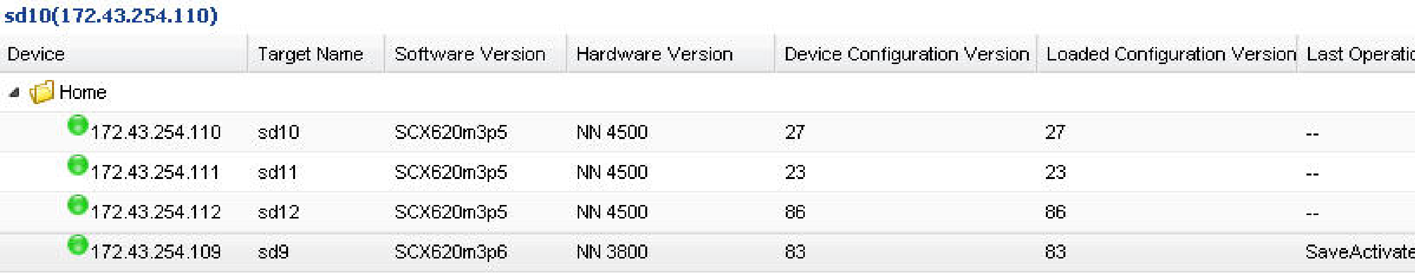
Using the Configuration Element Search

1. Click Search from any paged table in Configuration Manager.
   A dialog box appears.
2. Enter desired match values for any filters that appear in the dialog box.
3. Click Apply.
   The filtered search results appear in the table.

Note: To clear the filtered search results and return to the previous table, you must click Show All.

About Devices Data

The data in the Devices table provides at-a-glance information pertaining to your loaded device in Configuration Manager.



sd10(172.43.254.110)

Device	Target Name	Software Version	Hardware Version	Device Configuration Version	Loaded Configuration Version	Last Operatio
Home						
● 172.43.254.110	sd10	SCX620m3p5	NN 4500	27	27	--
● 172.43.254.111	sd11	SCX620m3p5	NN 4500	23	23	--
● 172.43.254.112	sd12	SCX620m3p5	NN 4500	86	86	--
● 172.43.254.109	sd9	SCX620m3p6	NN 3800	83	83	SaveActivate

The table explains the data shown.

Data	Description
Device	The device (or HA pair) in the device group
Target Name	User-defined name for each device
Software Version	Full release version, including patch number, of software on device
Hardware Version	Full hardware platform identification
Device Configuration Version	The device’s configuration version number. Note that until you load this device for the first time the device configuration number remains empty
Loaded Configuration Version	Configuration version number of the device’s configuration stored locally in the database If this column is blank, a configuration version has not been loaded for this managed device

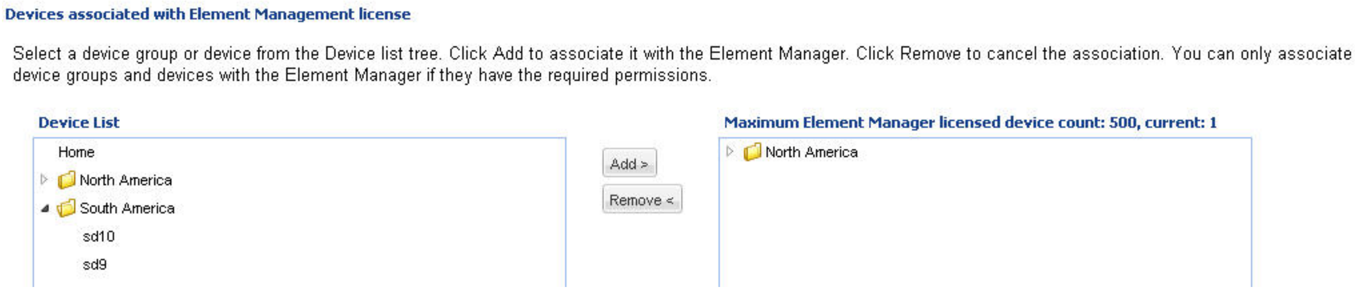
Data	Description
Last Operation	Last operation performed on this device
Status	The status of the last operation performed on this device
Status Change Time	The local date and time of the last status update change on the device.

Removing an Associated Device

You can remove a device from the Maximum Element Manager licensed device count table, thereby removing the association to the Element Manager license.

To remove a device from the Element Manager License:

1. Expand the Configuration Manager slider.
2. Click Devices. The Device table appears in the content area.
3. Click Add devices. The Devices associated with Element Manager license appears in the content area.
4. From the Device list, expand your device group folder and click the device you want to remove.
5. Click [Remove <] to move your device from the Maximum Element Manager licensed device count table back to the Device List.



Devices associated with Element Management license

Select a device group or device from the Device list tree. Click Add to associate it with the Element Manager. Click Remove to cancel the association. You can only associate device groups and devices with the Element Manager if they have the required permissions.

Device List

Maximum Element Manager licensed device count: 500, current: 1

Your device is removed from the Maximum Element Manager licensed device count table. If you remove the last device in a device group, the device group folder is also removed.

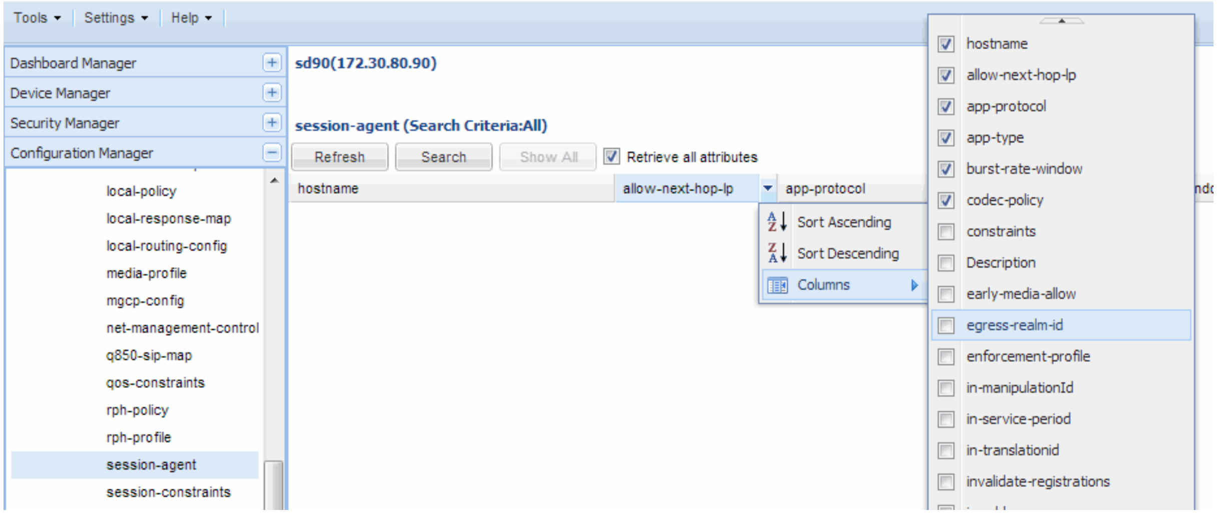
Optional Columns

Checking the Retrieve all attributes check box allows the system to collect all attributes other than non-required sub-element attributes and make them available alphabetically in the optional table columns.

Enabling Optional Columns

To enable the optional columns for multi-instance element tables:

1. Select the check box next to Retrieve all attributes to collect additional instance attributes and make them available as optional columns.



2. Select the drop-down arrow next to the column headers and navigate to Columns.
3. Select the check-boxes corresponding to the attributes you wish to display as additional columns in the table.

Offline Configuration

Offline configurations are configurations that can be applied to multiple devices, in order to share the same configuration data. An offline configuration is created by duplicating an existing managed device configuration or by selecting a schema from a supported software model.

Data variables allow network administrators to target elements that require device specific information, when duplicating an existing configuration. All data variables must have new values in order to push the configuration to a device.

Create an Offline Configuration

Configuration must be seeded from a supported software version schema or from an existing managed device configuration. Some attributes become enabled/disabled for editing, depending on the source of the offline configuration.

1. Expand Configuration Manager > Offline configuration.
2. Click Add.
3. Configuration name—Enter a unique name for the configuration.
4. Description—Enter a description for the configuration.
5. Offline configuration seeded from—Select the method for creating the configuration.
   - Software version—Creates an offline configuration from a supported software version schema.
   - Managed device—Creates an offline configuration by copying an existing managed device configuration.

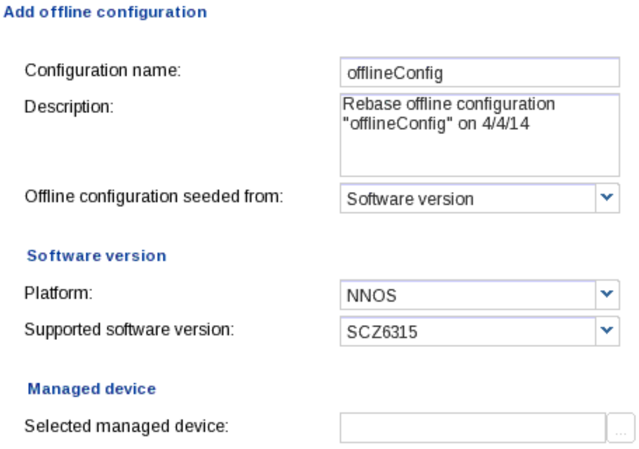
The following two parameters are only available for templates created from a selected software version.

6. Platform—Select the device hardware version in order to seed the configuration from a template.
7. Supported software version—Select the device software version in order to seed the configuration from a template.

The following parameter is only available for configurations seeded from an existing managed device.

8. Selected managed device—Click ... to launch the Selected managed device dialog.
9. Select a managed device from the device tree and click OK.
10. Click Apply.

Example Configuration



Add offline configuration

Configuration name: offlineConfig

Description: Rebase offline configuration "offlineConfig" on 4/4/14

Offline configuration seeded from: Software version

Software version

Platform: NNOS

Supported software version: SCZ6315

Managed device

Selected managed device:

Target Data Variables

Data variables are required in order to identify device-specific parameters for individual devices within a VM group. Each VM requires configuration of the boot loader and data variables before they are able to deploy. See the Oracle Communications Session Element Manager User Guide for more information on data variables and offline configuration.

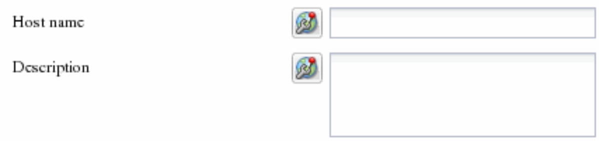
1. Expand Configuration Manager > Offline configuration.
2. Select a configuration from the table and click **Load**.
3. Click **OK** to dismiss the confirmation dialog.
   The selected configuration loads under Offline configuration.

Repeat the following steps for targeting a parameter as a Data Variable:

4. Navigate to the system element that requires configuration.
5. Click the icon in the upper-right corner and select the text box for the targeted attribute.
6. **Pre-populate from existing DV**— Select an existing data variable to pre-populate the following parameters.
7. **Name**— Enter an unique ID for the data variable.
8. **Label**— Enter a name for the data variable that appears in the individual VM configuration wizard.
9. **Description**— Enter a description for the data variable that appears in the tool-tip during configuration.
10. **Default value**— Enter a default value for the data variable.
11. Click **Add**.
12. Click **Apply** to submit configuration changes.
13. Click **Update** to push changes to the assigned devices.

Example Data Variables

An icon appears next to the parameters marked as data variables for individual device configuration.



Host name

Description

Configuration Archive

Oracle Communications Session Delivery Manager's Configuration archive lets you easily back up, restore, and manage your Net-Net SBC's configuration across multiple devices.

Configuration archive allows you to:

- Schedule back ups of device configurations
- Restore back ups of device configurations
- Apply a purge policy to devices and device groups, meaning you can delete archived configurations based on age or a set limit of backups

When configured for high availability, the Configuration archive exists on every node in a cluster. Whenever a configuration file is pulled from a device by a node, the file is sent to all of the nodes in the cluster.

Scheduling

When you select Configure archive from the Configuration Manager slider, the Schedules screen appears in the content area and displays all back ups run on the current date. To see all scheduled and past back ups, select Schedules from the Configuration Manager slider.

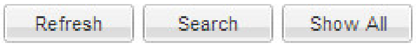
The Schedule Table

This table includes the following information for each device:

Backup Information	Description
Target	Device or device group's target name
Frequency	Interval at which back ups are scheduled
First Scheduled	Scheduled back up time and frequency
Last run time	Last time back up was performed
Device group	Group to which device belongs
Hardware version	Hardware platform on which device runs
Software version	Software version currently running on device

Performing Backup Tasks

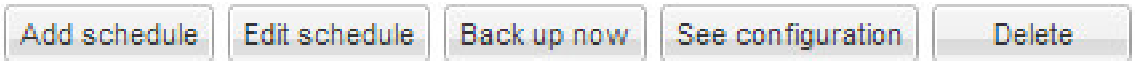
Action buttons appear at the top of the Schedules table:



This table describes the actions:

Action	Description
Refresh	Refreshes the contents of the Schedules table
Search	Launches the Backup search dialog, allowing you to filter the contents of the Schedules table
Show all	Clears all search criteria set by the Search dialog and displays all backed up configurations in the Schedules table

Action buttons that appear at the bottom of the Schedules table:



This table describes the actions.

Action	Description
Add schedule	Launches the Add schedules dialog, allowing you to select a time, frequency, and device(s) or device group(s) to backup
Edit schedule	Launches the Edit schedule dialog, allowing you to modify the backup schedule
Back up now	Backs up the configuration of the selected device or device group immediately
See configuration	Launches the Archive configuration screen showing only configurations associated with the backup selected
Delete	Deletes a row from the table. Deleted rows corresponding to a scheduled backup ceases

Archive Configurations Display

When you select the Configure archive option, all backed up configurations appears in the content area. To see all scheduled back ups, select Schedules from the Configuration Manager slider.

Configuration archives Table

This table describes the following information for each device:

Back up Information	Description
Configuration Name	Name of the configuration file
Source	Device's target name
Configuration Version	Version of the configuration
Hardware Version	Hardware platform on which device runs
Software Version	Software version currently running on device
Backup date	Date/time configuration was backed up

Backup Related Tasks

At the bottom of the Archive configurations table is a set of action buttons. For example:

This table describes the actions:

Action	Description
Rename	Launches the configuration name dialog, allowing you to modify the name of the backed up configuration
Restore	Restores the selected backup
Delete	Deletes selected configuration from the table

Creating and Restoring Backups

This section explains how to create and restore back ups of your Net-Net device configuration. You can schedule back ups to run once, daily, weekly, or monthly. You can also back up a configuration on demand.

When you restore a back up, you remove all edits made to the configuration after the back up was run.

When performing a configuration back up, the Net-Net SBC:

- Copies the configuration file into the ConfigBackups directory.
- Adds an entry to the database for the configuration file.
- Applies the set purge policy. Refer to the Managing Configuration Backups to set this policy.

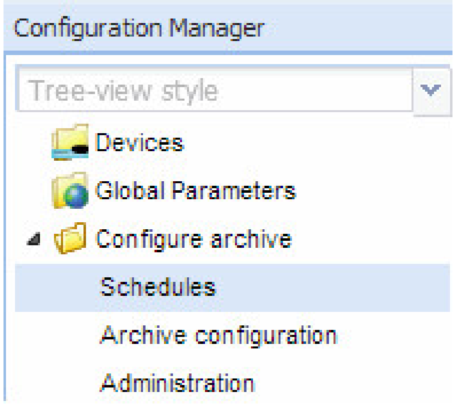
Backed up configurations are kept in the AcmePacket/ConfigBackups directory. A new directory is created for each device using the IP address in the location name.

Scheduling a Backup

You can schedule a backup to automatically archive the configuration of a device and/or device group.

To schedule a configuration backup:

1. Expand the Configuration Manager slider.



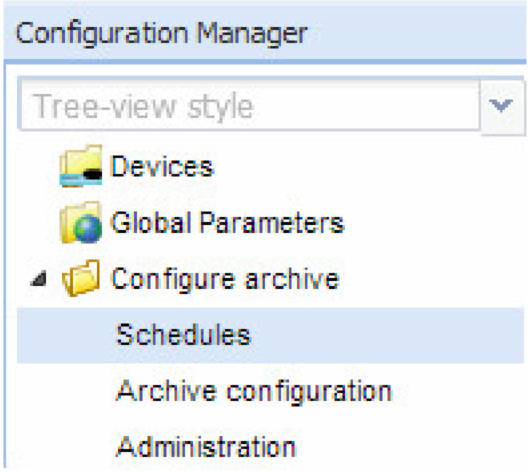
2. Expand Configure archive and click Schedules.
3. Click Add schedule. The Schedules screen appears.
4. Schedule—Select Schedule to set a date and time to back up a configuration.
5. Frequency—Select the frequency of configuration back ups from the combination box.
   - None—Do not repeat scheduled configuration back up.
   - Daily—Perform a daily scheduled configuration back up.
   - Weekly—Perform a weekly scheduled configuration back up.
   - Monthly—Perform a monthly scheduled configuration back up.
6. Start date—Choose a start date from the calendar.
7. Start time—Enter or select a start time.
8. Click the Devices tab.
9. Click Add. The Device selection dialog appears.
10. Select the device(s) or device group(s) you want to schedule a back up for.
11. Click Add >.
12. Click OK.
13. Click Apply to finalize the schedule.

Executing a Backup On Demand

You must add a device(s) and device group(s) to the schedules table before you can perform a back up. If you do not wish to have a reoccurring schedule, set the Schedule to On demand in the Add schedule dialog when scheduling a back up.

To perform a configuration backup on demand:

1. Expand the Configuration Manager slider.



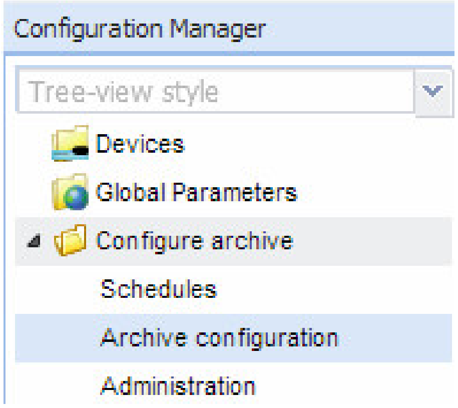
2. Expand Configure archive and click Schedules.
3. Click Add schedule. The Schedules screen appears.
4. Schedule—Select On demand to perform a configuration backup immediately.
5. Click the Devices tab.
6. Click Add. The Device selection dialog appears.
7. Select the device(s) or device group(s) you want to schedule a back up for.
8. Click Add >.
9. Click OK.
10. Click Apply to start the configuration backup on-demand.

Restoring a Backup

Restoring a backup is an on-demand process that you cannot schedule. Restoring a backup does not affect the purge policy or existing configuration backups.

To restore a configuration backup:

1. Expand the Configuration Manager slider.



2. Expand Configure archive and click Archive configuration.
3. Select a backed up configuration from the table and click Restore. A dialog appears.
4. Click Yes to restore the backed up configuration.

Managing Configuration Backups

Using Oracle Communications Session Delivery Manager’s tools, you can manage the configuration you have backed up. You can purge, search, or remove a backup. This section explains those operations.

Purge Policy

You can configure a purge policy to delete backed up configurations according to either an age limit or limit per device. Each time a configuration is backed up, a purge is performed according to the selected policy. You may only set one policy at a time, although you may run an on-demand purge at any point in time.

You can select either of the two following policies:

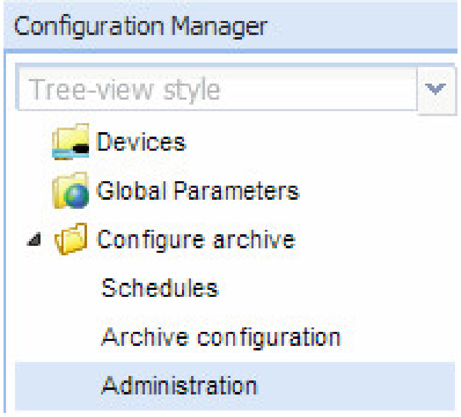
- Policy 1: A set number of archived configurations that should be kept per device. In this case, the oldest configurations are deleted first.
- Policy 2: You can set the number of days of daily, weeks of weekly, and months of monthly backed up configurations to keep.

Setting up a Purge Policy

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

To select a purge policy:

1. Expand the Configuration Manager slider.



2. Expand Configure archive and click Administration.
3. Please choose one of purge policy choices:—Select the purge policy you wish to set up and apply.

   To set up Policy 1:

   - Total Number of backup configurations to store per device—Enter a numerical value between 0 - 999999999.

   To set up Policy 2:

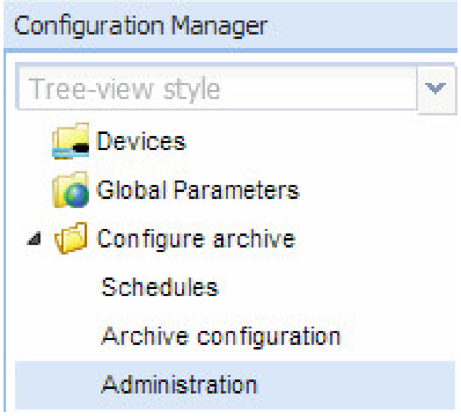
   - Deleting daily backup older than days—Enter a numerical value between 0 - 999999999. The default is 4 days.
   - Deleting weekly backup older than weeks—Enter a numerical value between 0 - 99999999. The default is 4 weeks.
   - Deleting monthly backup older than months—Enter a numerical value between 0 - 999999999. The default is 4 months.
4. Click Apply.

Executing an On-Demand Purge

When executing an on-demand purge, 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.

To execute an on-demand purge:

1. Expand the Configuration Manager slider.



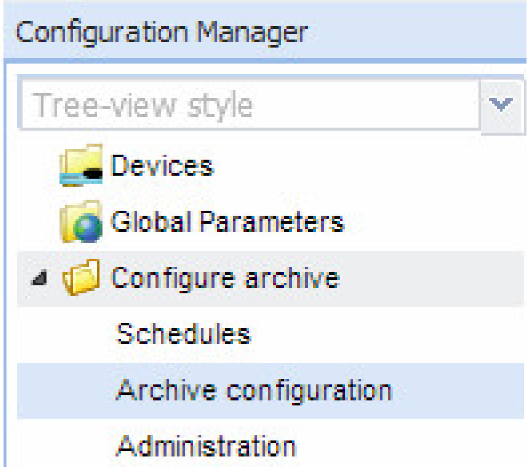
2. Expand Configure archive and click Administration.
3. Click the Operation tab.
4. Configuration archive purge policy—Select the scope of the purge.
   - Purge all archived configuration—Purges all files and configurations associated with selected device(s)/device group(s).
   - Purge per policy—Purges selected devices according to set purge policy.
5. Click the device group folder in which your device belongs to view the list of devices.
6. Select the target device or groups you wish to purge and click Add.
7. Click Purge.

Searching a Configuration

You can search the Configuration archive using one or more criteria.

To perform a search of a configuration:

1. Expand the Configuration Manager slider.



2. Expand Configure archive and click Archive configuration.
3. Click Search. The Configuration archive search dialog box appears.
4. Configuration name—Enter the name of a configuration.
5. Source—Enter the device’s target name.
6. Hardware version—Enter the platform version of a device.
7. Software version—Enter the software version of a device.
8. Start backup date—Choose a start time from the calendar.
9. End backup date—Choose an end time from the calendar.

10. Click OK to search using the configured criteria and close the dialog box.
11. Click Cancel to cancel your configured criteria and close the dialog box.

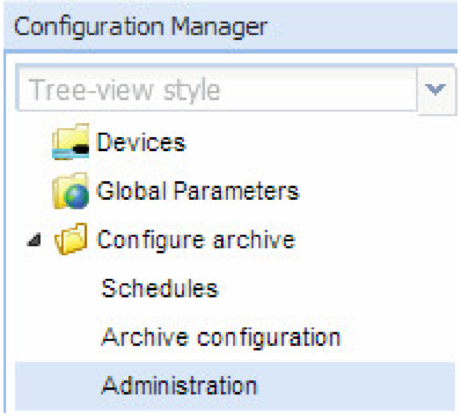
Changing the File Naming Policy

The names applied to archived configurations contain either the device's target name or IP address, followed by the date and time the configuration was downloaded from the device. You can select either the device's target name or IP address as the file naming policy. TARGET_NAME is selected by default.

For example, a configuration downloaded on February 14, 2012 at 1:08:15 PM is saved with the name sd231_2012_02_14_13_08_15.

To change the file naming policy:

1. Expand the Configuration Manager slider.



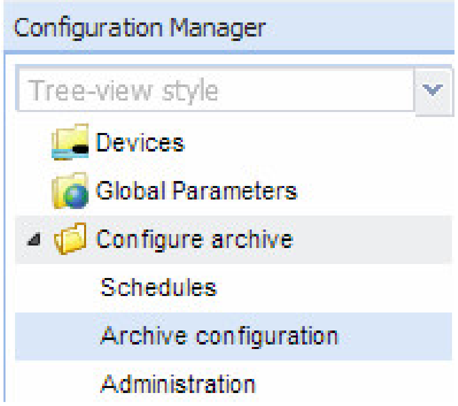
2. Expand Configure archive and click Administration.
3. Default configuration name settings—Select .
   - TARGET_NAME—Use the device's target name, followed by the date and time of the back up.
   - IP_ADDRESS—Use the device's IP address, followed by the date and time of the back up.
4. Click Apply.

Renaming a Configuration

You can rename of any backed up configuration to a more meaningful title in the Archive configuration screen. However, the actual file name on the system does not change and still adheres to the set file naming policy. The changed name of a configuration will only be displayed within Oracle Communications Session Delivery Manager.

To rename a configuration:

1. Expand the Configuration Manager slider.



2. Expand Configure archive and click Archive configuration.

3. Select the configuration you want to rename and click Rename.
4. Name—Enter the new name for the configuration.
5. Click OK to set the configuration name.

Administration

This section contains administrative information for the Configuration archive.

Audit Logs

The following operations are recorded in the Audit logs:

- Renaming of configurations
- Deletion of configurations
- Manual cleanup of the Configuration archive
- Administrative changes in cleanup policy or file naming policy
- Restoration of a configuration file
- Configuration backup

For more information about the audit trail, see the Oracle Communications Session Delivery Manager Administration Guide.

User Privileges

Depending on your user privilege level (or privileges set for the User Group to which you belong), you can perform certain operations in Configuration archive:

- Back up configurations
- Restore configurations
- Delete archived configurations
- Change Configuration archive settings

For more information about group/user privileges, see the Oracle Communications Session Delivery Manager Administration Guide.

Configuration Privileges

You can set one of two privilege levels for each level of operation in Configuration archive:

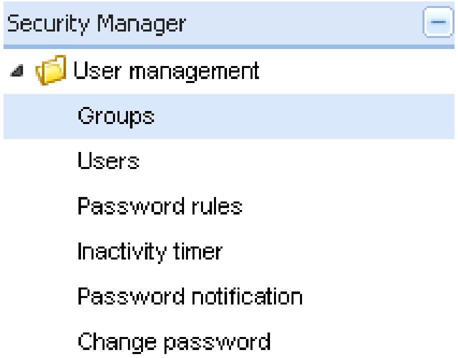
- Full—You can perform all actions associated with the selected Configuration archive operation. For example, you can back up, restore, or delete a configuration. All action buttons appear in the content area for the selected operations.
- None—You have no access to operations related to the Configuration archive. For example, you cannot back up, restore, or delete a configuration. Action buttons will be unavailable to click if you do not have privileges.

Setting Configuration Privileges

Before you can set their configuration privileges, a user must be added to a group under the Net-Net Security Manager.

To set configuration privileges for a user group:

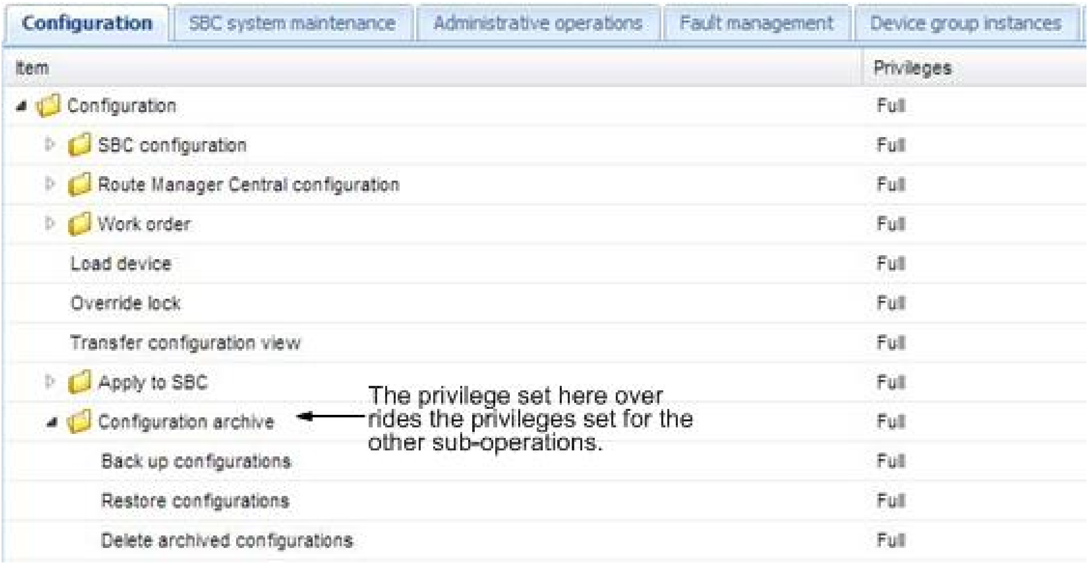
1. Expand the **Security Manager slider** > **User management**.



Security Manager

- User management
  - Groups
  - Users
  - Password rules
  - Inactivity timer
  - Password notification
  - Change password

2. Click Groups.
3. Select the group you want to set permissions for and click Edit.
4. Click the Configuration tab.
5. Expand the **Configuration** > **Configuration archive**.



Configuration | SBC system maintenance | Administrative operations | Fault management | Device group instances

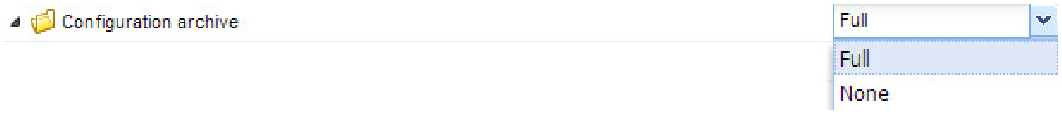
Item	Privileges
Configuration	Full
SBC configuration	Full
Route Manager Central configuration	Full
Work order	Full
Load device	Full
Override lock	Full
Transfer configuration view	Full
Apply to SBC	Full
Configuration archive	Full
Back up configurations	Full
Restore configurations	Full
Delete archived configurations	Full

The privilege set here over rides the privileges set for the other sub-operations.

The privileges are set according to the operation. With Full privileges assigned, users belonging to this group can:

- Configure archive: Back up, restore, or delete configurations on target device(s) or device group(s).
- Back up configurations: Back up configurations from target device(s) or device group(s).
- Restore configurations: Restore backed up configurations to the source device(s) or device group(s).
- Delete archived configurations: Delete backed up configurations from the archive.

6. Click the state in the Privileges column to change the privilege for this operation.



Configuration archive — Full

7. Click Apply. The privilege state is changed.

If the privilege state is set to None for an operation, the associated action buttons associated with this operation are invisible. For example, if set to None, the Add schedule, Edit schedule, Back up now, Restore, Delete actions will not be available to that user.

Administrative Privileges

You can set administrative privileges in Configuration archive. There are three privilege states for administrative operations:

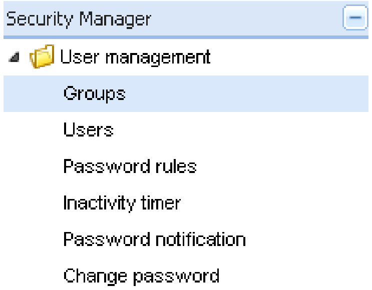
- Full—You can perform all actions associated with the selected Configuration archive operation, for example you can back up, restore, or delete a configuration. All action buttons appear in the content area for the selected operations.
- None—You have no access. For example, you cannot back up, restore, or delete a configuration.

Setting Administrative Privileges

Before you can set their administrative privileges, a user must be added to a group under the Net-Net Security Manager.

To set administrative privileges for a Group:

1. Expand the **Security Manager slider** > **User management**.



Security Manager

User management

Groups

Users

Password rules

Inactivity timer

Password notification

Change password

2. Click Groups.
3. Select the group you want to set permissions for and click Edit.
4. Click the Administrative operations tab.
5. Expand Administrative options.

   The privileges are set according to the operation. With Full privileges assigned, users belonging to this group can:

   - Change configuration archive settings: Set purge policies and change default settings such as the file naming policy.
6. Click the state in the Privileges column to change the privilege for this operation.
7. Click Apply.

3

Summary View

Overview

This chapter describes the data found in the summary view. Summary data for your managed devices is displayed here, such as, alarm status summary, key performance indicators, and a list of logged-in users.

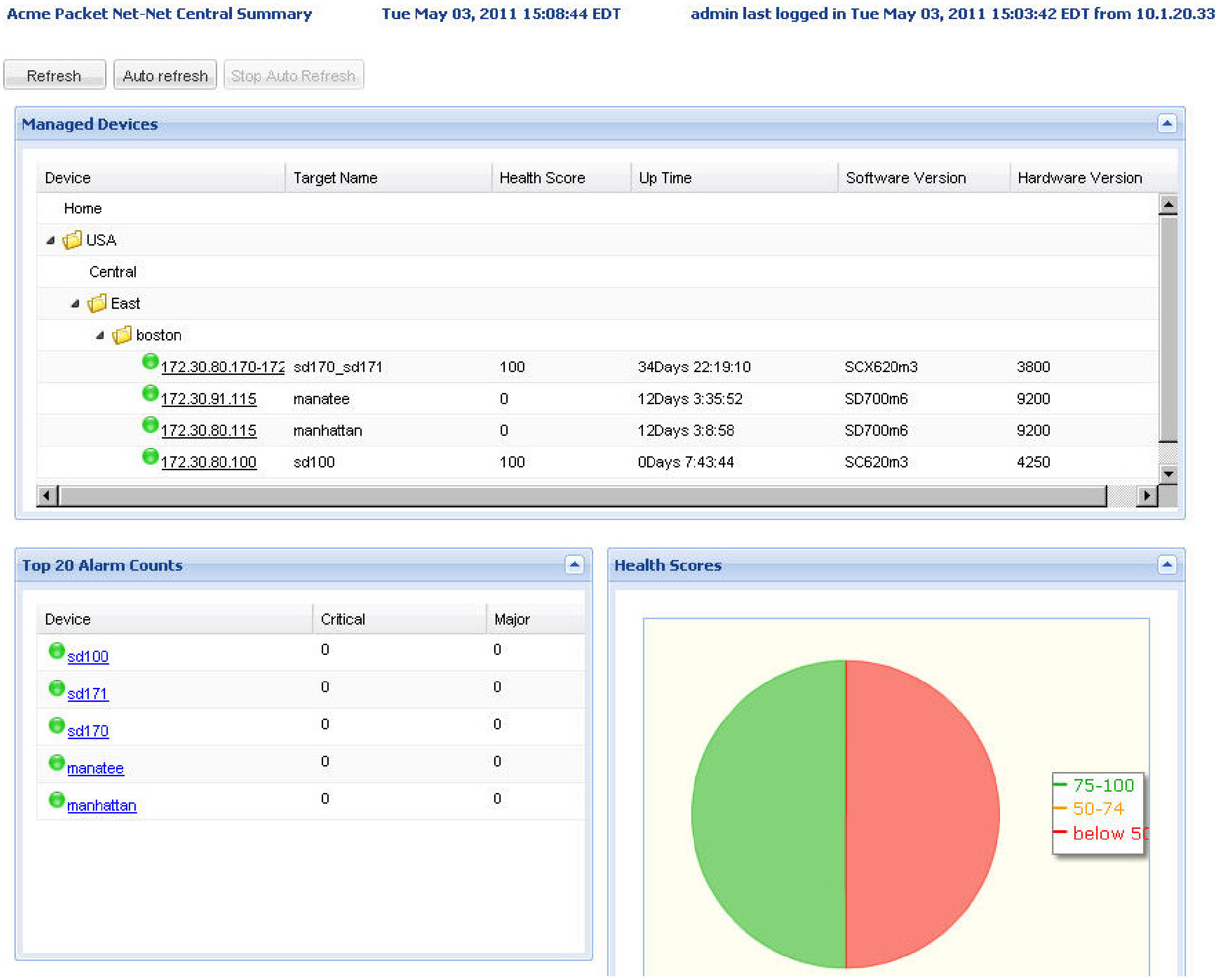
The information displayed is a combination of fault, performance, and other statistics gathered for the Net-Net SBC, and is displayed in a dashboard format. The information includes:

- Date and time of login
- Local date and time (with time zone adjustment) of the Oracle Communications Session Delivery Manager server
- A list of all devices by either IP address or host name
- Alarm status summary
- Key performance indicators (KPI): 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)

Summary View for Clusters

For clusters, the top-level displays and the device-specific summaries are shown for the active Net-Net SBC in the cluster. Statistics are not shown for the Net-Net SBC in standby mode.

Below is an example of the summary view display. You must scroll down in the content area to see all of the summary view data. The top of the content area contains a title bar with the current local time of the Oracle Communications Session Delivery Manager server and the IP address and time of the last successful login.



Acme Packet Net-Net Central Summary   Tue May 03, 2011 15:08:44 EDT   admin last logged in Tue May 03, 2011 15:03:42 EDT from 10.1.20.33

Managed Devices

Device	Target Name	Health Score	Up Time	Software Version	Hardware Version
Home					
USA					
Central					
East					
boston					
172.30.80.170-172	sd170_sd171	100	34Days 22:19:10	SCX620m3	3800
172.30.91.115	manatee	0	12Days 3:35:52	SD700m6	9200
172.30.80.115	manhattan	0	12Days 3:8:58	SD700m6	9200
172.30.80.100	sd100	100	0Days 7:43:44	SC620m3	4250

Top 20 Alarm Counts

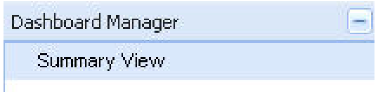
Device	Critical	Major
sd100	0	0
sd171	0	0
sd170	0	0
manatee	0	0
manhattan	0	0

Health Scores

Accessing Summary View Data

To access summary view data:

1. Expand the Dashboard Manager slider.
2. Click Summary View.



The summary view appears in the content area.

Refreshing Summary View Data

There are three buttons above the summary view tables: Refresh, Auto Refresh, and Stop Auto Refresh.

Refreshing Data

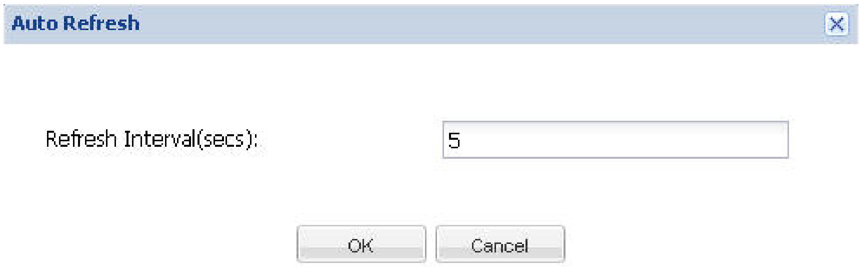
To refresh data:

Click Refresh to update the table data.

Configuring Auto Refresh

To configure auto refresh:

1. Click Auto refresh to configure a timed auto refresh interval. The Auto Refresh dialog box appears.
2. Refresh Interval(secs):—Enter the auto refresh interval in seconds.



Auto Refresh

Refresh Interval(secs): 5

3. Click OK. The page contents will update at the desired

Stopping Auto Refresh

To stop auto refresh:

- Click Stop Auto Refresh to cancel a configured auto refresh interval.

Note: If Auto refresh is configured, the Stop Auto Refresh button is enabled.

Summary View Displays

Summary view is broken into seven top-level displays:

- Managed Devices
- Top 20 Alarm Counts
- Health Scores
- Top 20 CPU Usage
- Top 20 Memory Usage
- Top 20 Call Rate
- Logged In Users

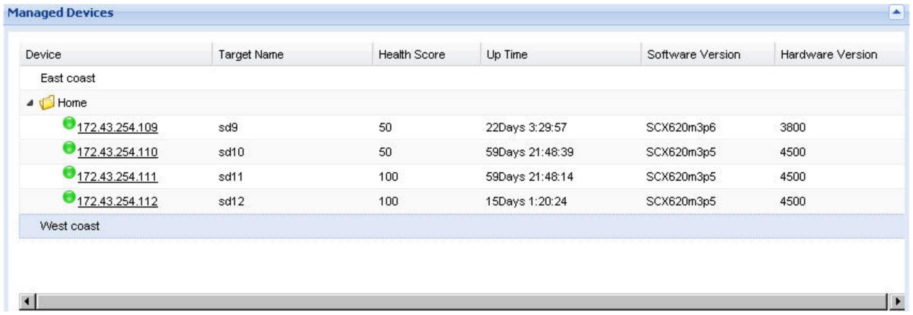
The following sections describe each top-level display.

Viewing Managed Devices Data

The Managed Devices table is the first table shown in the summary view content area.

To view managed devices data:

1. Expand the Dashboard Manager slider and click Summary View.
2. In the Managed Devices table, click the device group folder(s) to drill down to the device you want to view summary data for. The example below shows the devices found in the Home folder:.



Managed Devices

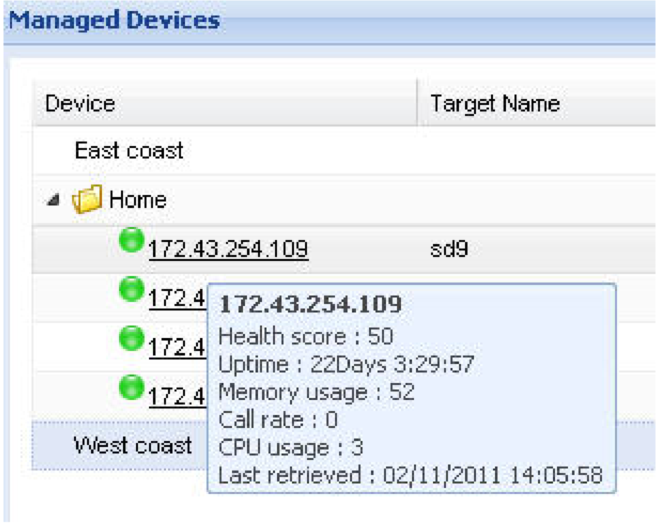
Device	Target Name	Health Score	Up Time	Software Version	Hardware Version
East coast					
Home					
172.43.254.109	sd9	50	22Days 3:29:57	SCX620m3p6	3800
172.43.254.110	sd10	50	59Days 21:48:39	SCX620m3p5	4500
172.43.254.111	sd11	100	59Days 21:48:14	SCX620m3p5	4500
172.43.254.112	sd12	100	15Days 1:20:24	SCX620m3p5	4500
West coast					

The following table describes the data displayed in the Managed Devices table.

Data	Description
Device	Managed device (or cluster) is displayed with an underline, which indicates you can click on the device to drill down for more summary data
Target Name	User-defined name for each device. An underscore (_) separates each target name for a cluster as in the example above, sd11_sd12
Health Score	System health percentage, with a system health percentage value of 100 (100%) being the healthiest
Up Time	System's up time in hours, minutes, and seconds
Software Version	Full release version, including patch number, of software on device
Hardware Version	Full hardware platform identification

3. Hover the mouse over a device for a pop-up with additional data for this device.

Below is an example of a pop-up for a standalone device:

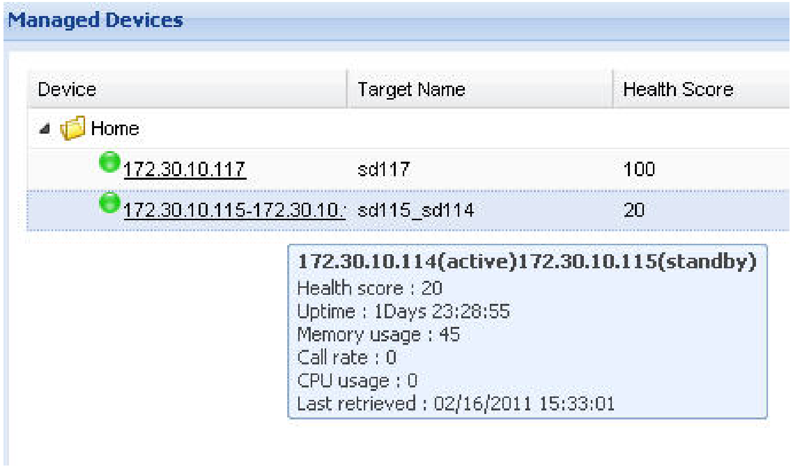


Managed Devices

Device	Target Name
East coast	
Home	
172.43.254.109	sd9
172.4	
172.4	
172.4	
West coast	

172.43.254.109
Health score : 50
Uptime : 22Days 3:29:57
Memory usage : 52
Call rate : 0
CPU usage : 3
Last retrieved : 02/11/2011 14:05:58

Below is an example of a pop-up for a cluster:



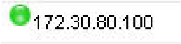
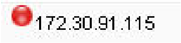
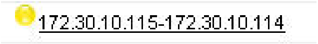
Managed Devices

Device	Target Name	Health Score
Home		
● 172.30.10.117	sd117	100
● 172.30.10.115-172.30.10.:	sd115_sd114	20

172.30.10.114(active)172.30.10.115(standby)
Health score : 20
Uptime : 1Days 23:28:55
Memory usage : 45
Call rate : 0
CPU usage : 0
Last retrieved : 02/16/2011 15:33:01

About Device Icons

A round, colored icon will appear to the left of your device in the Managed Devices table. This indicates whether or not the device is reachable by Oracle Communications Session Delivery Manager. If the icon is:

- Green: The device (or both devices in a cluster) is reachable by Oracle Communications Session Delivery Manager and information for this device can be retrieved through SNMP.
- 
  ● 172.30.80.100
- Red: Oracle Communications Session Delivery Manager cannot currently contact the device (or cannot contact both devices in a cluster).
- 
  ● 172.30.91.115
- Yellow: The standby device in the cluster is not reachable by Oracle Communications Session Delivery Manager.
- 
  ● 172.30.10.115-172.30.10.114

Viewing KPI, Alarms, and License Data

You can access key performance indicators, alarms, and license information by drilling down within the Managed Devices table.

To view KPI, alarms, and license data:

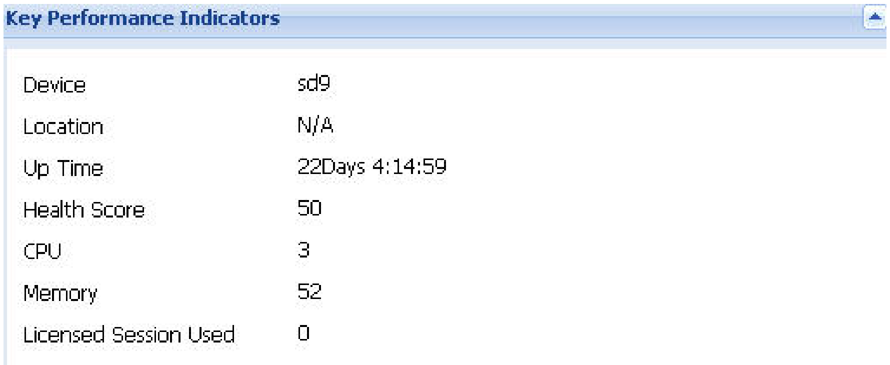
1. Expand the Dashboard Manager slider and click Summary View.
2. In the device column of the managed devices table, click the device you want to view key performance indicators, alarm summary, and license information for. The Key Performance Indicators (KPI) table appears first.

   There are three buttons above the KPI table:

   - Refresh—Updates the table contents
   - Back—Returns to the main summary view display
   - View Alarms—Navigates away from the devices summary view and to the alarm data under Fault Manager. For an explanation of alarms information, see Alarms.

Viewing Key Performance Indicators

The Key Performance Indicators table displays the following information for your device.



Key Performance Indicators

Device	sd9
Location	N/A
Up Time	22Days 4:14:59
Health Score	50
CPU	3
Memory	52
Licensed Session Used	0

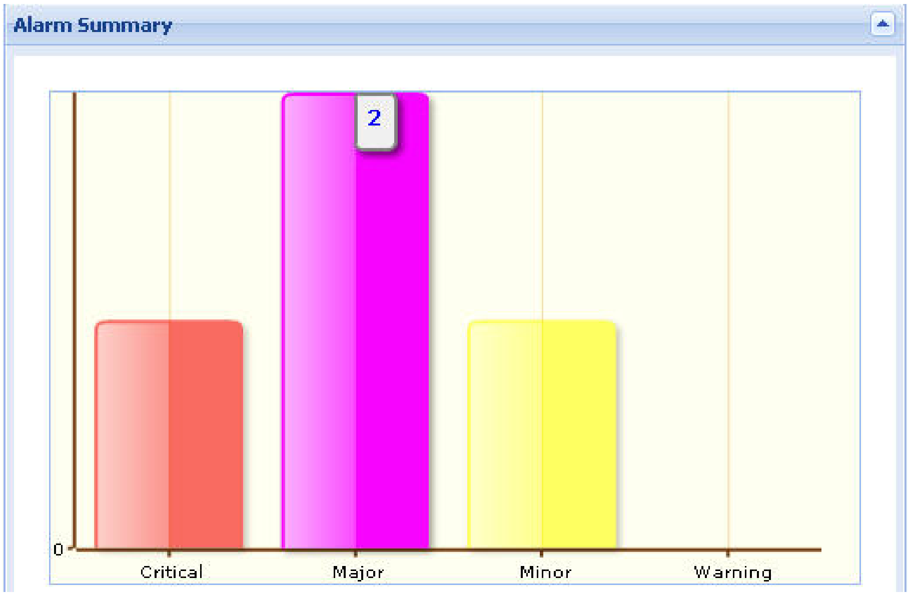
The following table describes the data displayed.

Data	Description
Device	The device managed by Oracle Communications Session Delivery Manager and for which the data is retrieved via 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, current signaling sessions

Note: For D-series systems, the CPU reflects the CPU of the card (NPU or SPU) with the highest CPU usage in the Net-Net SBC.

Viewing Alarm Summary

The Alarm Summary table displays a bar chart of the alarm counts for all alarm categories for your device. Mouse over a bar within the chart for the number of alarms that bar represents. For example:



The system-default alarm colors for each alarm severity are:

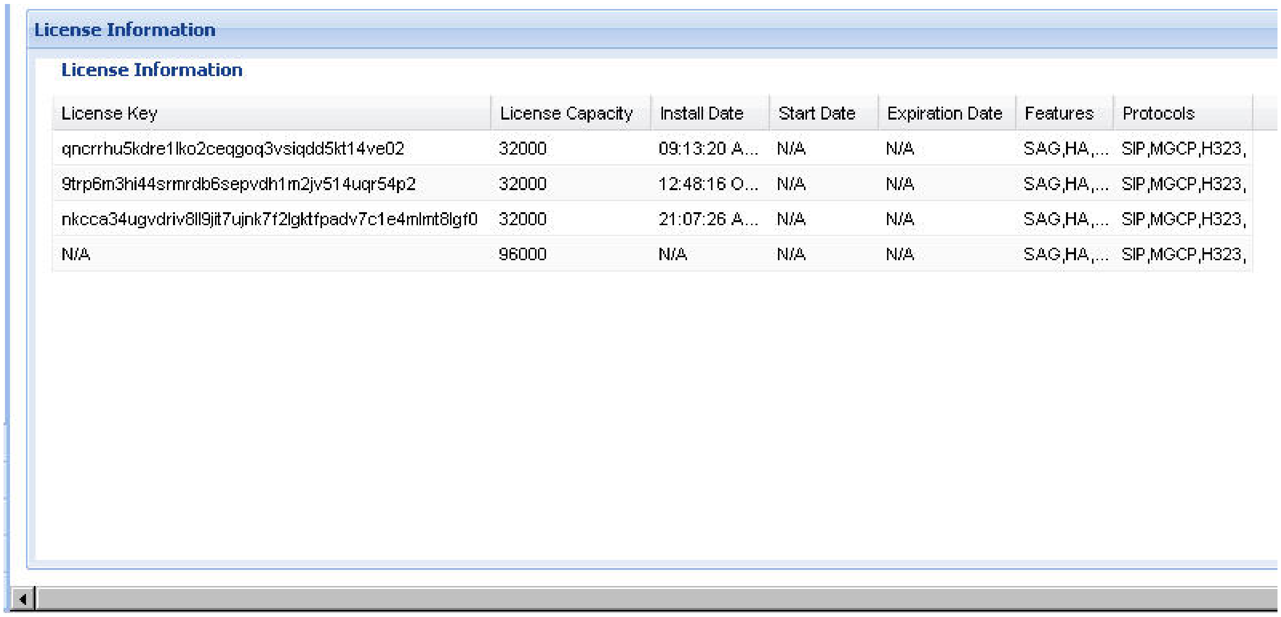
- Critical: Red
- Major: Orange
- Minor: Yellow
- All other alarms: Green

You can customize alarm colors for each severity level. See Alarm Severity Color-Coding for more information.

In the example above, the major alarm color has been changed from orange to dark pink.

Viewing License Information

The License Information table displays the following information.



License Information

License Information

License Key	License Capacity	Install Date	Start Date	Expiration Date	Features	Protocols
qncrrhu5kdre1lko2ceqgoq3vsiqdd5kt14ve02	32000	09:13:20 A...	N/A	N/A	SAG,HA,...	SIP,MGCP,H323,
9trp6m3hi44srmrdb6sepvdh1m2jv514uqr54p2	32000	12:48:16 O...	N/A	N/A	SAG,HA,...	SIP,MGCP,H323,
nkcca34ugvdriv8ll9jit7ujnk7f2lgktfpadv7c1e4mlmt8lgf0	32000	21:07:26 A...	N/A	N/A	SAG,HA,...	SIP,MGCP,H323,
N/A	96000	N/A	N/A	N/A	SAG,HA,...	SIP,MGCP,H323,

The data is defined as follows.

Data	Description
License Key	License number for this device
License Capacity	Maximum number of simultaneous sessions allowed by the Net-Net system for all combined protocols
Install Date	Installation time and date in the following format: hh:mm:ss, month, day, year. Displays N/A if license is not enabled
Start Date	Start time and date in the following format: hh:mm:ss, month, day, year. Displays N/A if license is not enabled
Expiration Date	Expiration time and date in the following format: hh:mm:ss, month, day, year. Displays N/A if license is not enabled
Features	All features licensed for this device. Values are: Interworking (IWF) Quality of Service (QoS) Acme Control Protocol (ACP) Local Policy (LP)

Data	Description
	Session Agent Group (SAG) ACC (Allows the Net-Net system to create connections and send CDRs to one or more RADIUS servers) High Availability (HA)
Protocols	All protocols licensed for this device. Values are: SIP MGCP H.323

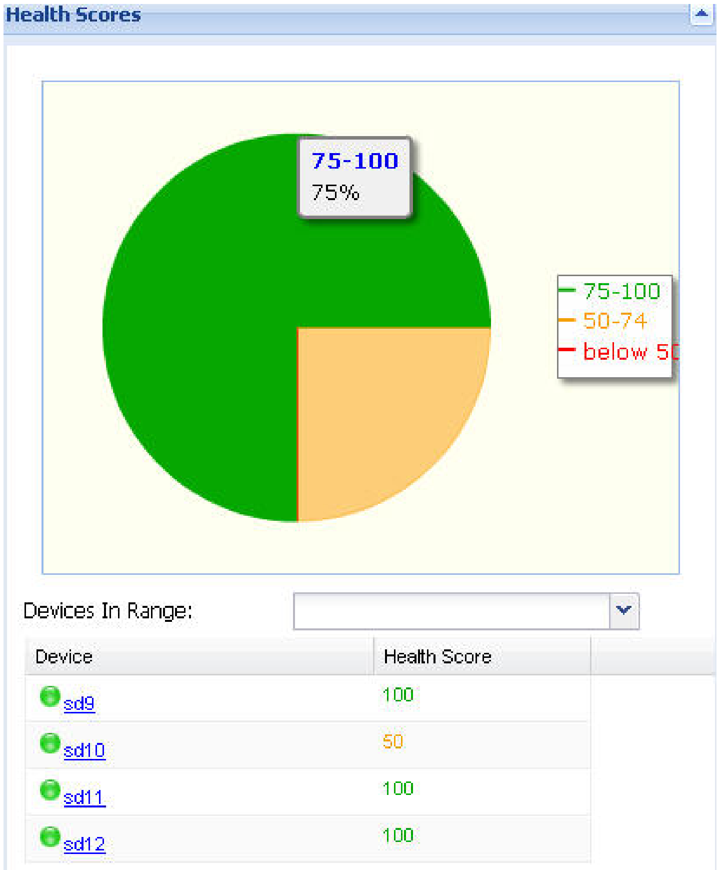
Viewing Health Scores Data

The Health Scores display provides a pie chart of health scores for your devices.

To view the health score data for a device:

1. Expand the Dashboard Manager slider and click Summary View. Health Scores displays the health scores for your devices.

   When you mouse over the pie chart a pop-up provides a health score percentage for all your devices. For example:.



Devices In Range:

Device	Health Score
● sd9	100
● sd10	50
● sd11	100
● sd12	100

2. Hover the mouse over a device in the Device list for a popup with additional data for this device.

Health Score Ranges

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

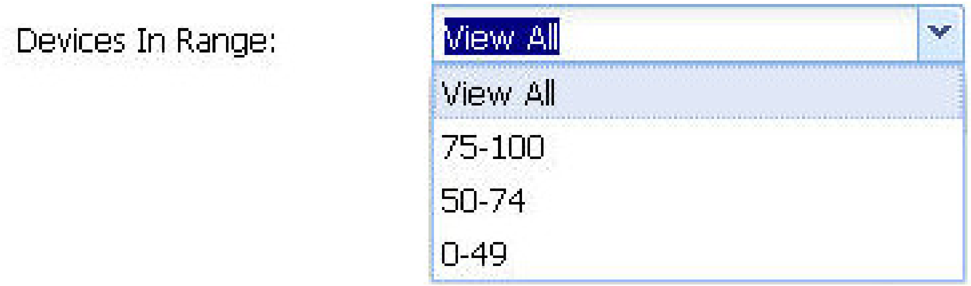
- Green: Indicates a score range from 75 to 100, inclusive
- Orange: Indicates a score range from 50 to 74, inclusive
- Red: Indicates a score below 50

Customizing the Health Score Range Display

You can customize the health score range display. By setting the Devices in range parameter, you can select the range of devices you want to view health scores for.

To customize the health score range display:

1. From the Health Scores chart, scroll to Devices In Range.
2. Devices In Range—Click the range you want to apply in the drop down list.



The display automatically adjusts to the health score range you select. The default range is View All.

The following table describes the data displayed.

Data	Description
Device	The device managed by Oracle Communications Session Delivery Manager and for which the data is retrieved via an SNMP query
Health Score	The health score for this device. The health score range is 0 to 100 per cent. Health scores lower than 60 indicate the device is in poor health

Viewing Top 20 Memory Usage

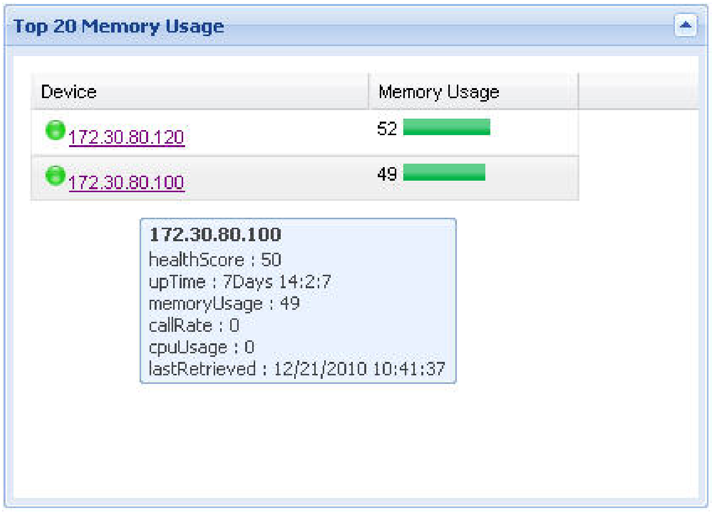
The Top 20 Memory Usage table appears on the summary view window and displays a summary of the top 20 devices currently using the most memory (by percentage).

Note: For D-series systems, the summary view reflects the memory usage of the card (NPU or SPU) with the highest memory usage in the Net-Net SBC.

To view the top 20 memory usage data for a device:

1. Expand the Dashboard Manager slider and click Summary View.

   The Top 20 Memory Usage table is sorted by descending percentage of memory used.
2. Hover the mouse over the device name for a popup with additional data for this device.



Device	Memory Usage
172.30.80.120	52
172.30.80.100	49

172.30.80.100
healthScore : 50
upTime : 7Days 14:2:7
memoryUsage : 49
callRate : 0
cpuUsage : 0
lastRetrieved : 12/21/2010 10:41:37

The following table describes the data displayed.

Data	Description
Device	The device managed by Oracle Communications Session Delivery Manager and for which the data is retrieved via an SNMP query
Memory Usage	Percentage of memory used

The Memory Usage column displays a numerical value of the memory utilization in percentage, followed by a colored bar, which corresponds with the memory usage percentage. The greater the percentage, the longer the bar.

The Memory Usage bar is represented in two colors:

- Red: Indicates memory usage is between 90% and 100%
- Green: Indicates memory usage is below 90%

Viewing Top 20 CPU Usage

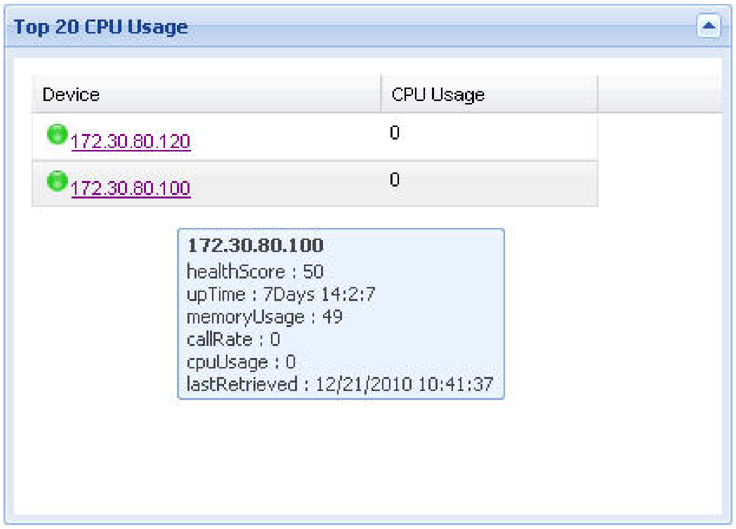
The Top 20 CPU Usage table appears on the summary view window and displays a summary of the top 20 devices with the highest CPU utilization.

Note: For D-series systems, the summary view reflects the CPU usage of the card (NPU or SPU) with the highest CPU usage in the Net-Net SBC.

To view the top 20 CPU usage data for a device:

1. Expand the Dashboard Manager slider and click Summary View.

   The Top 20 CPU Usage table is sorted by descending percentage of CPU used.
2. Hover the mouse over the device name for a popup with additional data for this device.



Top 20 CPU Usage

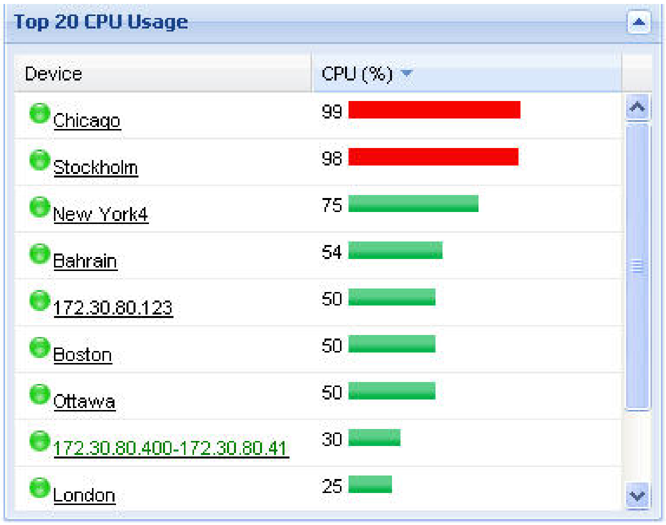
Device	CPU Usage
172.30.80.120	0
172.30.80.100	0

172.30.80.100
healthScore : 50
upTime : 7Days 14:2:7
memoryUsage : 49
callRate : 0
cpuUsage : 0
lastRetrieved : 12/21/2010 10:41:37

The following table describes the data displayed.

Data	Description
Device	The device managed by Oracle Communications Session Delivery Manager and for which the data is retrieved via an SNMP query
CPU Usage	Percentage of CPU utilization

The CPU Usage column displays a percentage value of the CPU utilization followed by a colored bar, which corresponds with the CPU percentage. The greater the percentage, the longer the bar. For example:



Top 20 CPU Usage

Device	CPU (%)
Chicago	99 🟥
Stockholm	98 🟥
New York4	75 🟩
Bahrain	54 🟩
172.30.80.123	50 🟩
Boston	50 🟩
Ottawa	50 🟩
172.30.80.400-172.30.80.41	30 🟩
London	25 🟩

The CPU Usage bar is represented in two colors:

- Red: Indicates CPU usage is between 90% and 100%
- Green: Indicates CPU usage is below 90%

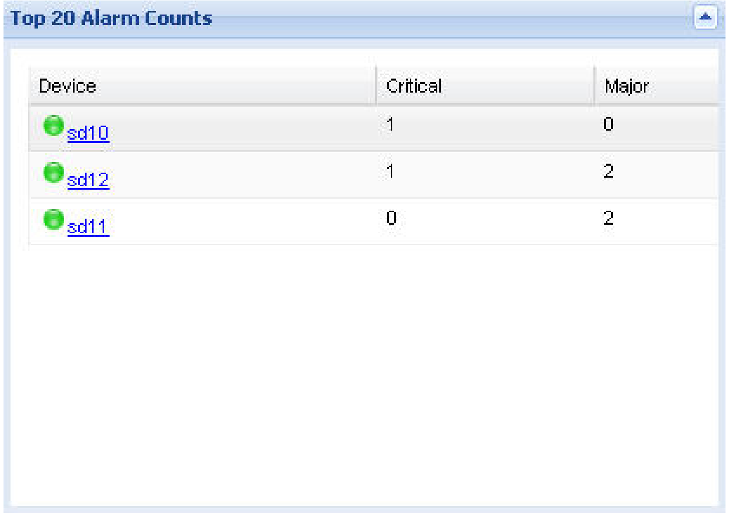
Viewing Top 20 Alarm Counts

The Top 20 Alarm Counts displays a summary of the top 20 alarms with a critical or major designation. The summary displays the number of critical and/or major alarms generated. Click Refresh to refresh the data or you can configure Auto refresh to set a refresh interval in seconds.

To view the top 20 alarm counts for a device:

1. Expand the Dashboard Manager slider and click Summary View.

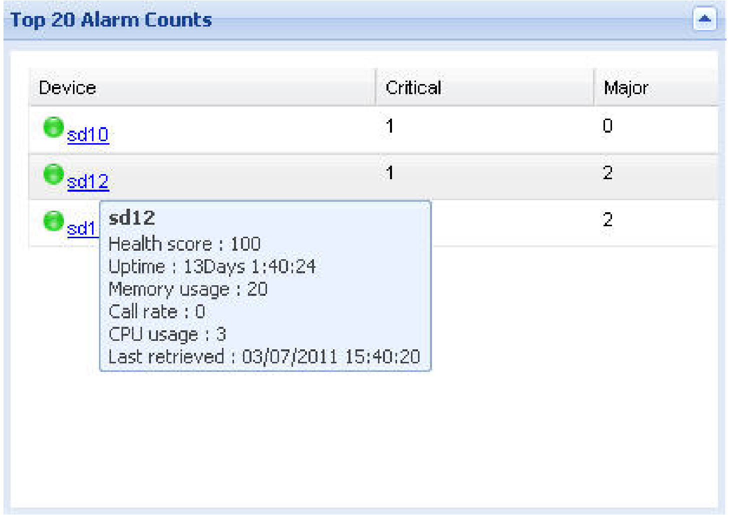
   The Top 20 Alarm Counts display appears in the lower left corner of the content area and displays the top 20 alarms with critical and major designations.



Top 20 Alarm Counts

Device	Critical	Major
● sd10	1	0
● sd12	1	2
● sd11	0	2

2. Hover the mouse over the device for a popup with additional data for this device.



Top 20 Alarm Counts

Device	Critical	Major
● sd10	1	0
● sd12	1	2
● sd1		2

sd12
Health score : 100
Uptime : 13Days 1:40:24
Memory usage : 20
Call rate : 0
CPU usage : 3
Last retrieved : 03/07/2011 15:40:20

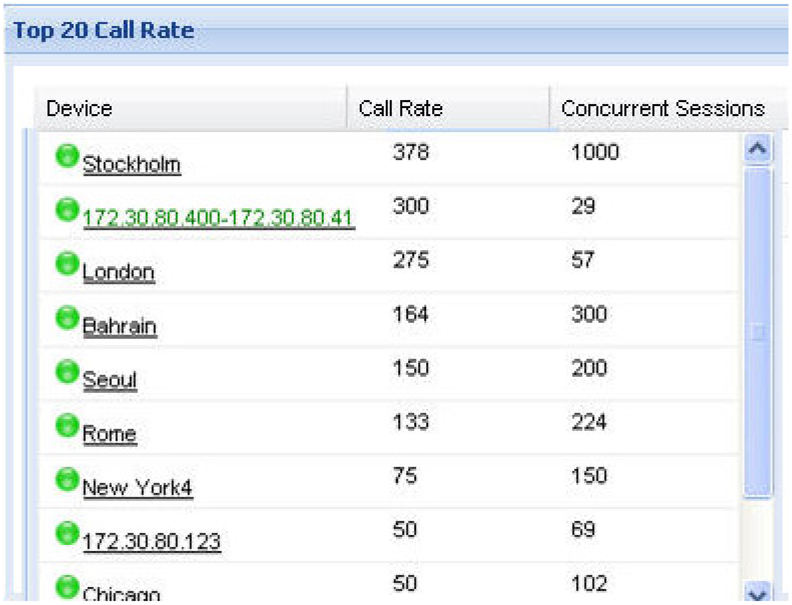
Note: The data refreshes only when auto refresh is configured or when refresh button is clicked.

Viewing Top 20 Call Rate

The Top 20 Call Rate table appears on the summary view window and displays a summary of the top 20 devices with the highest calls-per-second rate.

To view the top 20 call rate data for a device:

Expand the Dashboard Manager slider and click Summary View.



Top 20 Call Rate

Device	Call Rate	Concurrent Sessions
Stockholm	378	1000
172.30.80.400-172.30.80.41	300	29
London	275	57
Bahrain	164	300
Seoul	150	200
Rome	133	224
New York4	75	150
172.30.80.123	50	69
Chicago	50	102

The following table describes the data displayed.

Data	Description
Device	The device managed by Oracle Communications Session Delivery Manager and for which the data is retrieved via an SNMP query
Call Rate	The number of active calls for each device
Concurrent Sessions	The number of concurrent sessions for each device

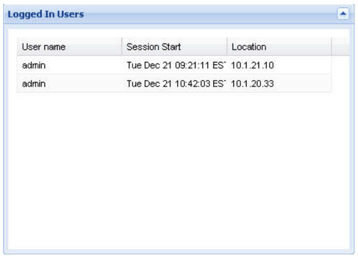
Viewing Logged In Users

With appropriate privileges, you can view the Logged In Users table. It appears on the summary view window and displays a list of all users currently logged into Oracle Communications Session Delivery Manager. The list will not display if you do not have administration-level privileges.

To view the list of logged in users:

Expand the Dashboard Manager slider and click Summary View.

The names within the Logged In Users table are sorted in ascending alphanumeric order by default.



Logged In Users

User name	Session Start	Location
admin	Tue Dec 21 09:21:11 ES	10.1.21.10
admin	Tue Dec 21 10:42:03 ES	10.1.20.33

The following table describes the data displayed.

Data	Description
User Name	Name of the user logged in to Oracle Communications Session Delivery Manager

Summary View

Data	Description
Session Start	The time the user logged in to Oracle Communications Session Delivery Manager
Location	The IP address of the user’s system

4

Viewing the Audit Log

Overview

This chapter explains how to view the audit log. The audit log provides information about the changes made using the Oracle Communications Session Delivery Manager. Audit trails enable you to view all operations that have been performed, the time they were performed, whether they were successful and who performed them.

Logged Information

Information is logged for the following operations:

- Login user
- Logout user
- Adding managed devices
- Adding device groups
- Loading Net-Net SBCs
- Adding an element
- Modifying an element
- Deleting elements
- Rebooting
- Switching HA pair roles
- Saving configurations
- Activating configurations
- Saving and activating configurations

Audit Trail Information

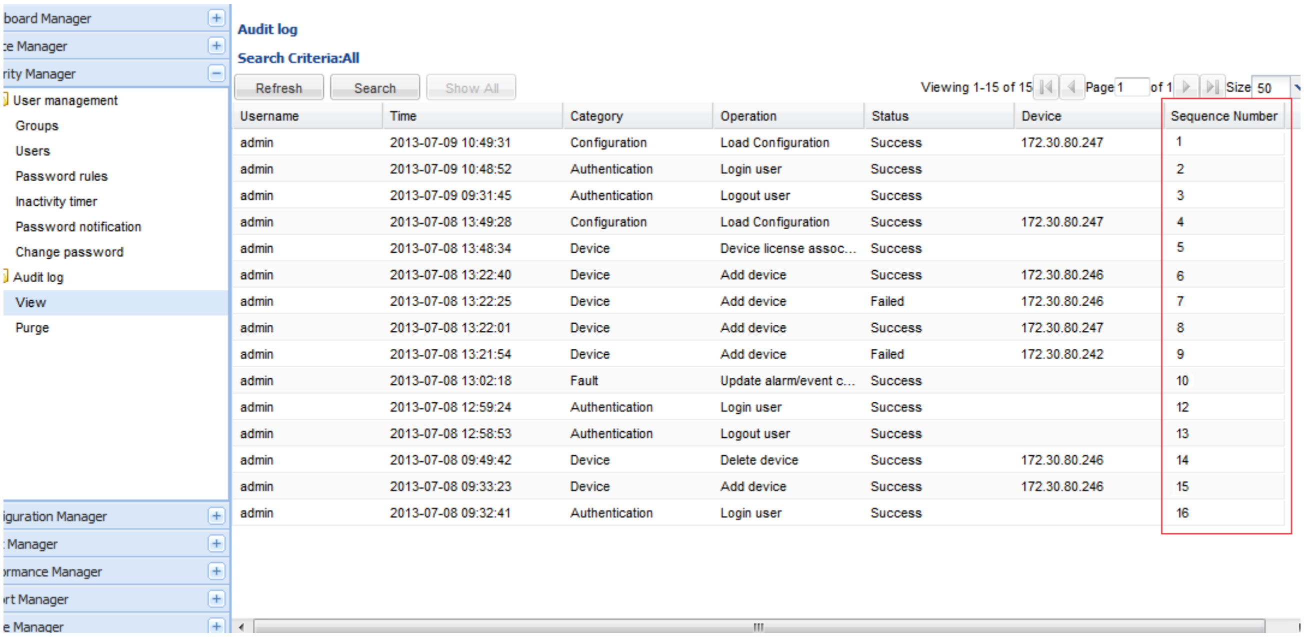
Audit trails include the following information:

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

Sequential Numbering

Sequential Numbers

Sequential numbers are generated for device-specific audit logs with a number. Each log entry generates a new sequential number ranging from 1-2^64 to display in the Audit log table. Numbers are not unique across clusters and cannot be referenced between different machines. You must enable the hidden Sequential number column to view it in the Audit Log table.



Audit log

Search Criteria:All

Viewing 1-15 of 15

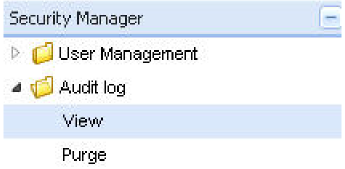
Username	Time	Category	Operation	Status	Device	Sequence Number
admin	2013-07-09 10:49:31	Configuration	Load Configuration	Success	172.30.80.247	1
admin	2013-07-09 10:48:52	Authentication	Login user	Success		2
admin	2013-07-09 09:31:45	Authentication	Logout user	Success		3
admin	2013-07-08 13:49:28	Configuration	Load Configuration	Success	172.30.80.247	4
admin	2013-07-08 13:48:34	Device	Device license assoc...	Success		5
admin	2013-07-08 13:22:40	Device	Add device	Success	172.30.80.246	6
admin	2013-07-08 13:22:25	Device	Add device	Failed	172.30.80.246	7
admin	2013-07-08 13:22:01	Device	Add device	Success	172.30.80.247	8
admin	2013-07-08 13:21:54	Device	Add device	Failed	172.30.80.242	9
admin	2013-07-08 13:02:18	Fault	Update alarm/event c...	Success		10
admin	2013-07-08 12:59:24	Authentication	Login user	Success		12
admin	2013-07-08 12:58:53	Authentication	Logout user	Success		13
admin	2013-07-08 09:49:42	Device	Delete device	Success	172.30.80.246	14
admin	2013-07-08 09:33:23	Device	Add device	Success	172.30.80.246	15
admin	2013-07-08 09:32:41	Authentication	Login user	Success		16

Accessing Audit Logs

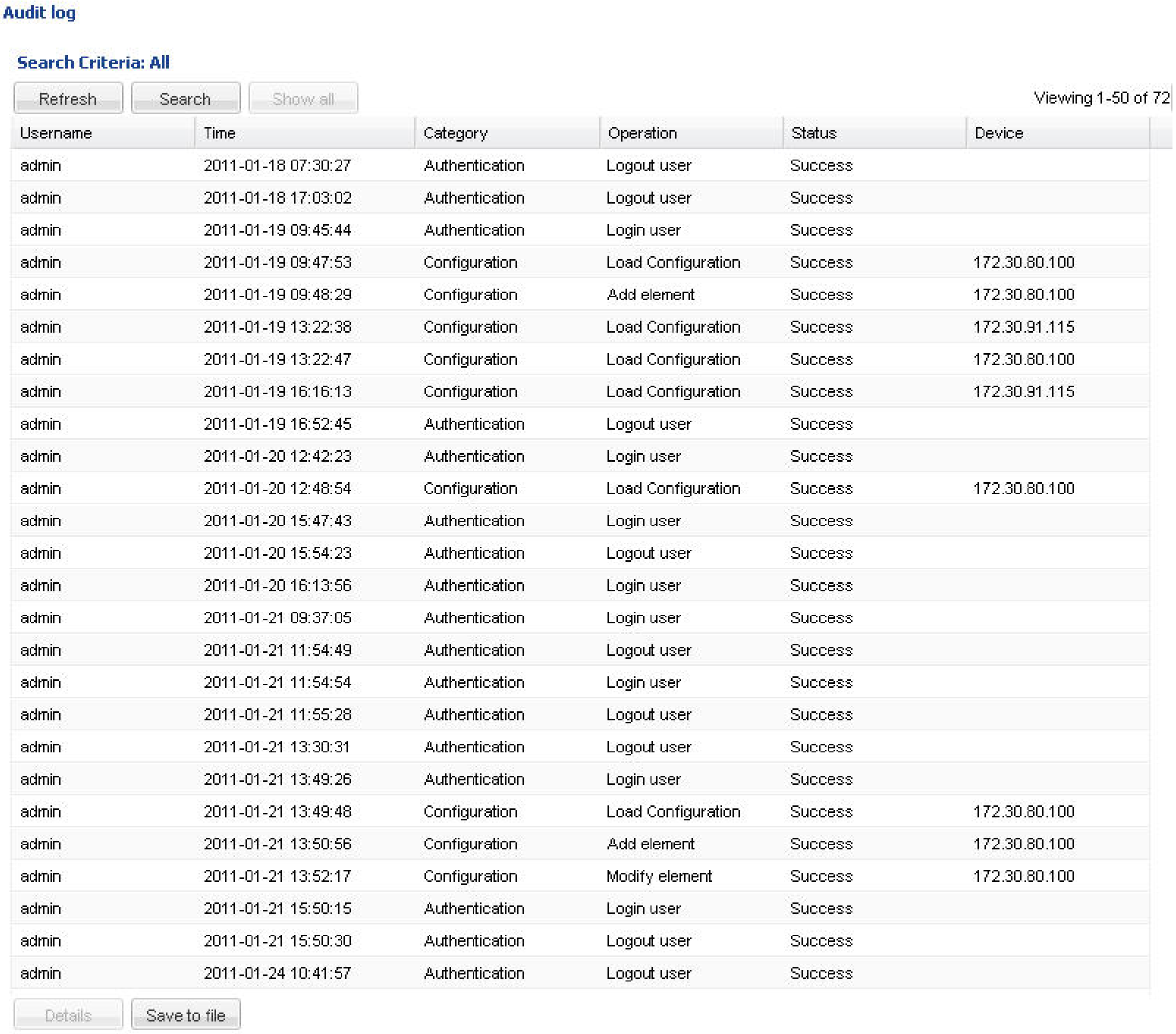
This section explains how to access the audit log's data. All users can access the Audit logs from the Security Manager slider, under Audit log.

To access audit logs:

1. Expand the Security Manager slider and click Audit log to expand the folder.

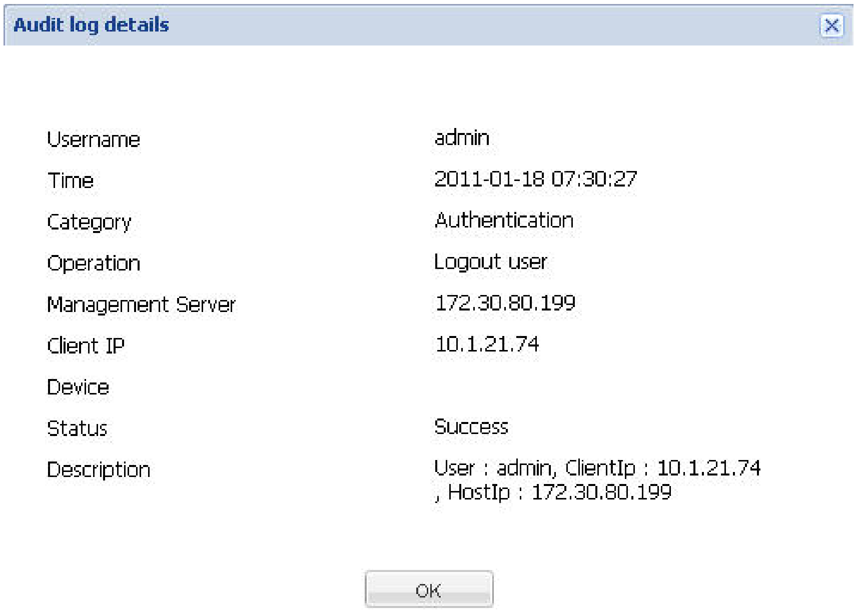


2. Click View. The Audit log table appears in the content area. For example:



Username	Time	Category	Operation	Status	Device
admin	2011-01-18 07:30:27	Authentication	Logout user	Success	
admin	2011-01-18 17:03:02	Authentication	Logout user	Success	
admin	2011-01-19 09:45:44	Authentication	Login user	Success	
admin	2011-01-19 09:47:53	Configuration	Load Configuration	Success	172.30.80.100
admin	2011-01-19 09:48:29	Configuration	Add element	Success	172.30.80.100
admin	2011-01-19 13:22:38	Configuration	Load Configuration	Success	172.30.91.115
admin	2011-01-19 13:22:47	Configuration	Load Configuration	Success	172.30.80.100
admin	2011-01-19 16:16:13	Configuration	Load Configuration	Success	172.30.91.115
admin	2011-01-19 16:52:45	Authentication	Logout user	Success	
admin	2011-01-20 12:42:23	Authentication	Login user	Success	
admin	2011-01-20 12:48:54	Configuration	Load Configuration	Success	172.30.80.100
admin	2011-01-20 15:47:43	Authentication	Login user	Success	
admin	2011-01-20 15:54:23	Authentication	Logout user	Success	
admin	2011-01-20 16:13:56	Authentication	Login user	Success	
admin	2011-01-21 09:37:05	Authentication	Login user	Success	
admin	2011-01-21 11:54:49	Authentication	Logout user	Success	
admin	2011-01-21 11:54:54	Authentication	Login user	Success	
admin	2011-01-21 11:55:28	Authentication	Logout user	Success	
admin	2011-01-21 13:30:31	Authentication	Logout user	Success	
admin	2011-01-21 13:49:26	Authentication	Login user	Success	
admin	2011-01-21 13:49:48	Configuration	Load Configuration	Success	172.30.80.100
admin	2011-01-21 13:50:56	Configuration	Add element	Success	172.30.80.100
admin	2011-01-21 13:52:17	Configuration	Modify element	Success	172.30.80.100
admin	2011-01-21 15:50:15	Authentication	Login user	Success	
admin	2011-01-21 15:50:30	Authentication	Logout user	Success	
admin	2011-01-24 10:41:57	Authentication	Logout user	Success	

3. Click ▶ to page forward through the data.
4. Click ▶| to move to the last page of data.
5. Click Save to file (at bottom of screen) to save it to a file locally.
6. Click Refresh (at top of screen) to refresh the data in the audit log.
7. Click a row in the Audit log table and click Details. The Audit log details window appears.



Username	admin
Time	2011-01-18 07:30:27
Category	Authentication
Operation	Logout user
Management Server	172.30.80.199
Client IP	10.1.21.74
Device	
Status	Success
Description	User : admin, ClientIp : 10.1.21.74 , HostIp : 172.30.80.199

Audit trails include the following information:

- Name of the user who performed the operation
- Time the operation was performed by the user
- Category of operation performed by the user
- Specific operation performed by the user
- Address of the management server accessed
- IP address of the client that was used
- Device the user performed operation upon
- Status of the operation performed by the user, whether it was successful or failed
- Description of the operation

8. Click OK to exit the window.

Searching the Audit Log

You can search the audit log using one or more criteria.

To search the audit log:

1. Click the Search button. The Audit Log Search dialog box appears.

2. Username:—Choose a user name from the drop-down list.

3. Category:—Choose a category from the drop-down list.

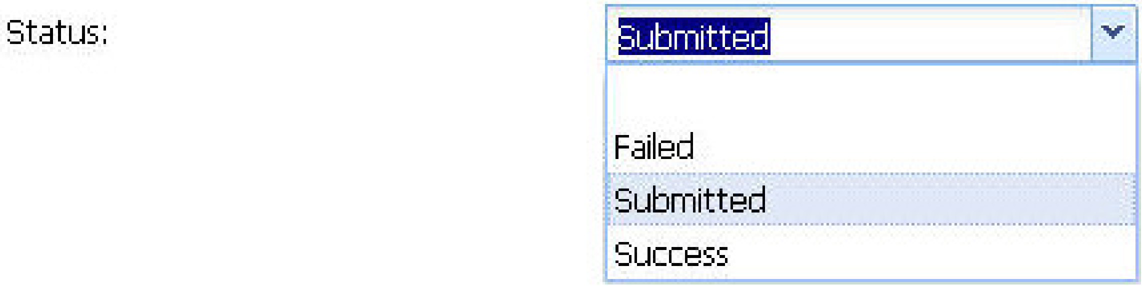
4. Operation:—Choose an operation from the list.

5. Management Server:—Enter the IP address of a management server.

6. Client IP:—Enter the IP address of a client.

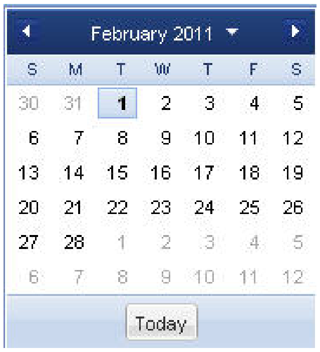
7. Device:—Enter a device IP address.

8. Status:—Choose an operation status from the drop-down list.



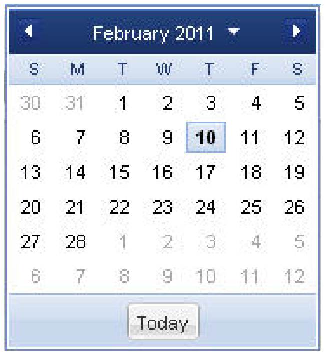
Status: Submitted

9. Start Time:—Choose a start time from the calendar.



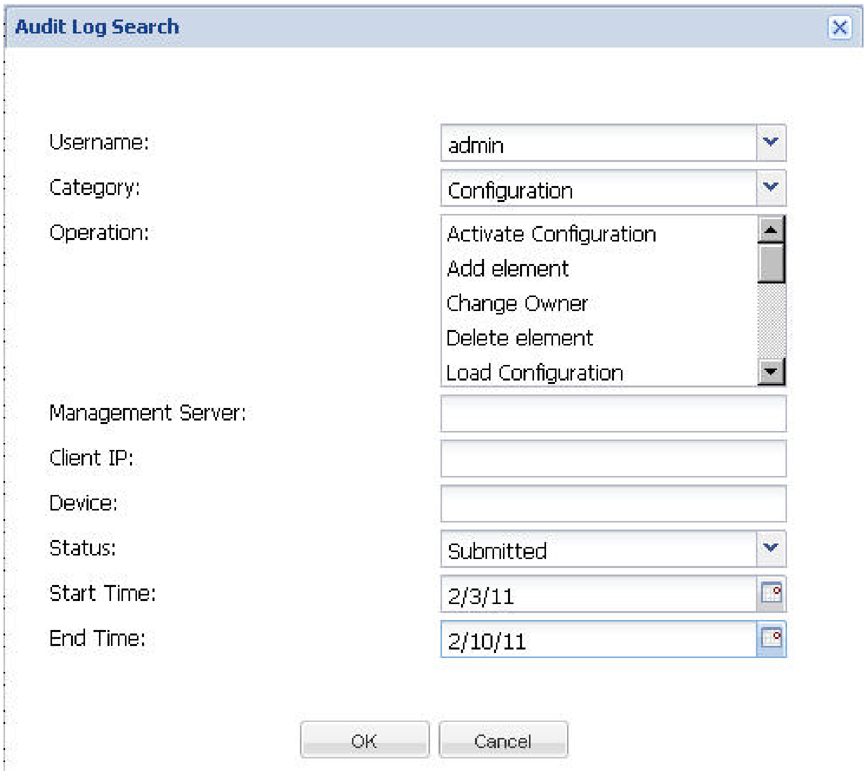
S	M	T	W	T	F	S
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5
6	7	8	9	10	11	12

10. End Time:—Choose an end time from the calendar.



S	M	T	W	T	F	S
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5
6	7	8	9	10	11	12

An example of the search criteria is below.



Audit Log Search

Username: admin

Category: Configuration

Operation:
Activate Configuration
Add element
Change Owner
Delete element
Load Configuration

Management Server:

Client IP:

Device:

Status: Submitted

Start Time: 2/3/11

End Time: 2/10/11

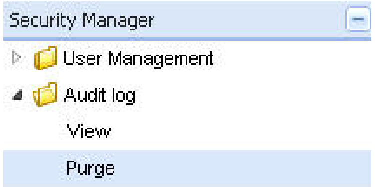
11. Click OK in the Audit Log Search dialog box to search using the configured criteria.
12. Click Show All in the Audit log display to show all audit log entries.

Purging Audit Log Files

If you have the permission assigned, you can configure the number of days of audit logs to keep. You can also manually purge audit logs.

To purge audit log files:

1. Expand the Security Manager slider.
2. Click Audit log to expand the folder.



3. Click Purge. Purge audit logs appears in the content area.
4. Interval in days:—Enter the number of days for which you want to keep audit logs.

Interval in days: 7

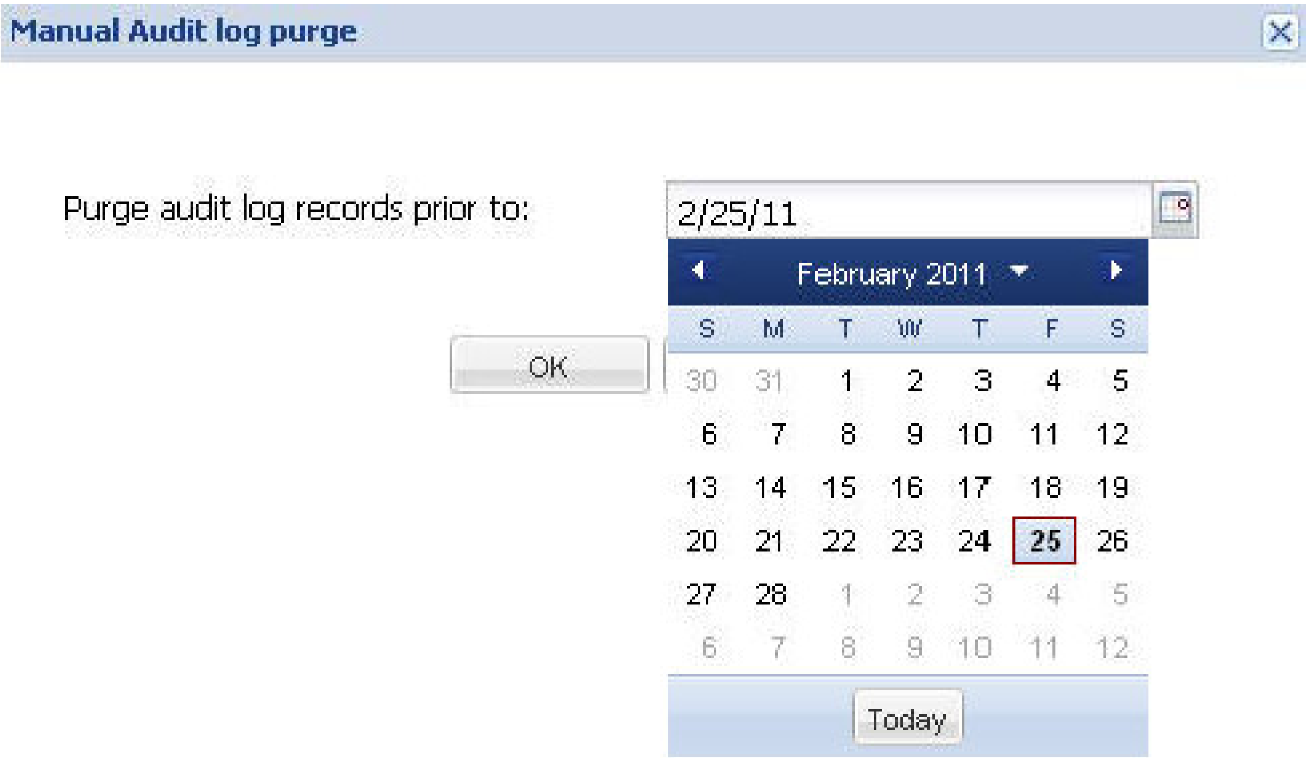
5. Click Apply.

Manually Purging

To manually purge audit logs:

1. With the purge audit log information displayed in the content area, click Purge. The Manual Audit log purge dialog box appears.

2. Purge audit log records prior to:—Choose the date from the calendar prior to which you want audit logs purged.



Manual Audit log purge

Purge audit log records prior to: 2/25/11

3. Click OK.

5

Viewing Fault Information

Overview

This chapter contains information about fault manager using Oracle Communications Session Delivery Manager. Fault manager involves the following:

- Events
- Alarms
- Trap event settings

The information about events and alarms is based on the Oracle® standard and proprietary Management Information Bases (MIBs). For more information about the events, alarms, and MIBs, see the Net-Net MIB Reference Guide. For information about Net-Net SBC logging, see the Logs chapter in the Oracle Communications Session Delivery Manager 4000 Configuration Guide.

Relationship of Traps to Events and Alarms

All SNMP traps from nodes managed by Oracle Communications Session Delivery Manager appear as events in the Events window of the Fault Manager slider. Only a subset of traps are considered to be alarms, which appear in the Alarms window of the Fault Manager slider. (Summary information about alarms can be viewed in the Summary View window of the Dashboard Manager slider.) In general, the Oracle Communications Session Delivery Manager characterization of alarms matches that of the Net-Net SBC. See the Net-Net MIB Reference Guide for more information.

Verifying Net-Net SBC Configuration

You should verify that the Net-Net SBCs for which you want to view fault manager information have the following information configured:

- Simple Network Management Protocol (SNMP) communities
- MIB contact
- Trap receivers

  These features are necessary to use Oracle's Oracle Communications Session Delivery Manager to manage Net-Net SBCs. They provide important monitoring and system health information that contribute to a robust deployment of the Net-Net system.

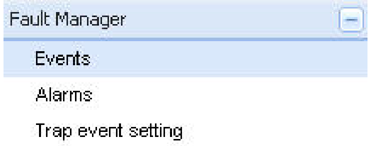
See the System Configuration chapter of the Oracle Communications Session Delivery Manager 4000 Configuration Guide for complete information about these parameters.

Accessing Fault Manager

This section explains how to access the Net-Net SBC fault information displayed by Oracle Communications Session Delivery Manager.

To access fault manager information:

Click the plus sign (+) next to Fault Manager to expand the slider. The slider expands to include Events, Alarms, and Trap event setting.



From here you can choose the type of information you want to view. Click Events, Alarms, or Trap event setting. The following sections describe the data found in the Fault Manager slider.

Events

This section explains how to access and view event information. Events are caused by actions that generate one or more of the following:

- Alarms
- Entries in a log file
- SNMP traps

For more information about events, refer to the Net-Net MIB Reference Guide.

Event Severity

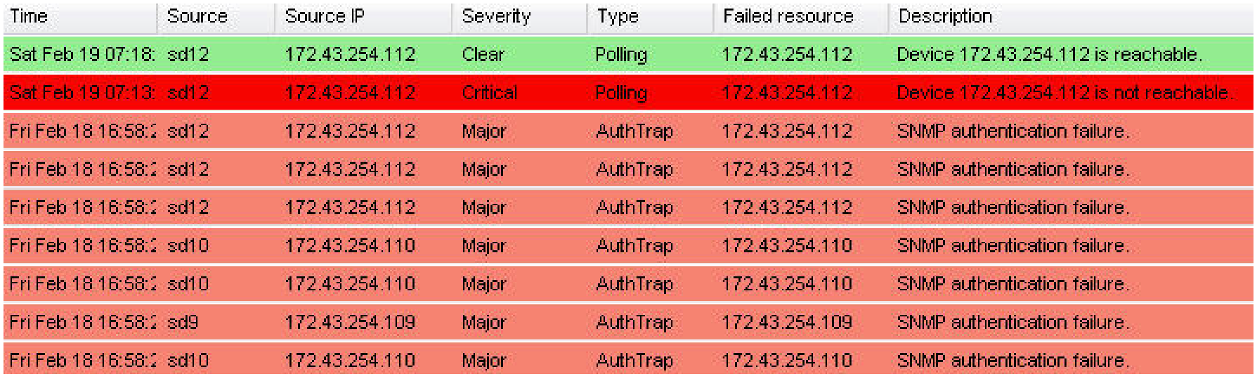
There are eight severity levels ranging from the highest Emergency to the lowest severity of Debug.

Numerical Code	Severity Types	Severity Label
0	Emergency (system is unusable)	EMERGENCY (0)
1	Alert (action must be taken immediately)	CRITICAL (1)
2	Critical (critical conditions)	MAJOR (2)
3	Error (error conditions)	MINOR (3)
4	Warning (warning conditions)	WARNING (4)
5	Notice (normal but significant condition)	NOTICE (5)
6	Informational (informational messages)	INFO (6)
7	Debug (debug level messages)	TRACE (7) DEBUG (8) DETAIL (9)

Accessing Events Information

To access events information:

Expand the Fault Manager slider and click Events. The list of network events appears in the content area.



Time	Source	Source IP	Severity	Type	Failed resource	Description
Sat Feb 19 07:18:	sd12	172.43.254.112	Clear	Polling	172.43.254.112	Device 172.43.254.112 is reachable.
Sat Feb 19 07:13:	sd12	172.43.254.112	Critical	Polling	172.43.254.112	Device 172.43.254.112 is not reachable.
Fri Feb 18 16:58:2	sd12	172.43.254.112	Major	AuthTrap	172.43.254.112	SNMP authentication failure.
Fri Feb 18 16:58:2	sd12	172.43.254.112	Major	AuthTrap	172.43.254.112	SNMP authentication failure.
Fri Feb 18 16:58:2	sd12	172.43.254.112	Major	AuthTrap	172.43.254.112	SNMP authentication failure.
Fri Feb 18 16:58:2	sd10	172.43.254.110	Major	AuthTrap	172.43.254.110	SNMP authentication failure.
Fri Feb 18 16:58:2	sd10	172.43.254.110	Major	AuthTrap	172.43.254.110	SNMP authentication failure.
Fri Feb 18 16:58:2	sd9	172.43.254.109	Major	AuthTrap	172.43.254.109	SNMP authentication failure.
Fri Feb 18 16:58:2	sd10	172.43.254.110	Major	AuthTrap	172.43.254.110	SNMP authentication failure.

The following table defines the information displayed on the events page.

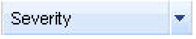
Event Category	Description
Time	Date and time this event was generated
Source	Exact source of the event
Source IP	Source IP address of the event
Severity	User-defined severity level for this event: Critical Major Minor Clear Warning Info Notice Trace Debug Unknown
Type	Type of trap associated with this event
Failed resource	Resource responsible for the event
Description	Short textual description of the event

Customizing the Table Display

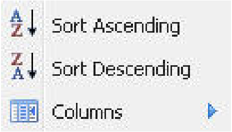
You can customize the data presented in all tables found in Fault Manager by changing the columns that are displayed and/or the order of the table entries.

To customize the table display:

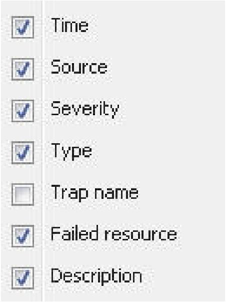
1. Position the cursor over a column heading. An arrow appears on the right hand side of the box. For example:



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



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



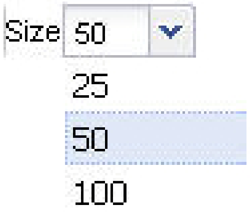
5. Click a marked checkbox to hide that column or click an empty checkbox to display that column.
6. Click elsewhere in the display to clear the menus.

Changing Number of Items on the Page

By default, 50 items are shown per page. You can change the number of items viewed for all tables in Fault Manager.

To change the number of items displayed:

1. At the top of the Network events window, click the down arrow next to Size. The drop down list of values appears.

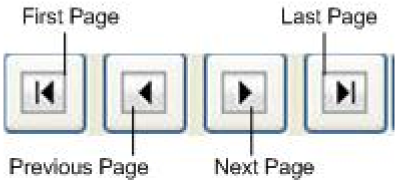


2. Click the number you want to apply.

Navigating Pages

To navigate through multiple pages:

1. Use the navigation arrows located at the top of the Network events window to navigate through multiple pages.
2. Click the navigation icons to display the desired page, such as the first page, previous page, next page, and the last page of Events list view.



Filtering Event Data

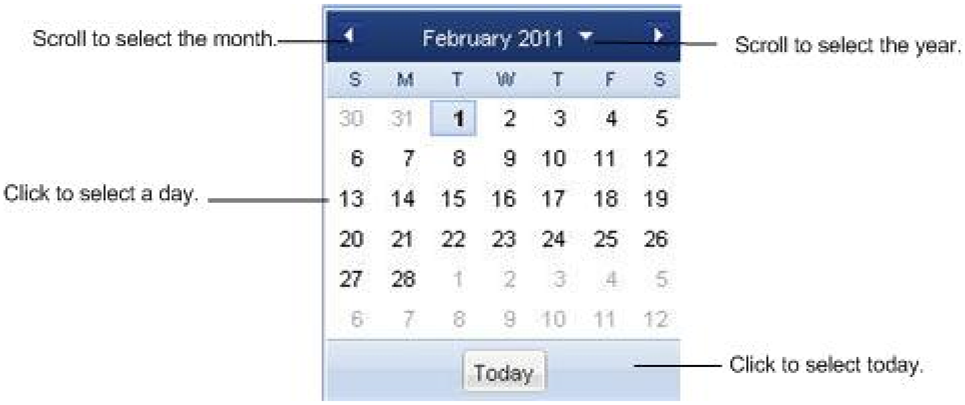
You can filter event data based on date range, source IP, severity, type, and trap name. You can filter information for one or more of the criterion.

To filter event data:

1. Expand the Fault Manager slider and click Events. The events data appears in the content area.
2. Click Search. The Filter search dialog box appears.
3. Date from:—Click to access the Calendar.

   Choose the month and the year by using the arrows to scroll to the needed options.

   Choose the day by clicking the appropriate cell or by clicking Today..



Scroll to select the month.

Scroll to select the year.

Click to select a day.

Click to select today.

Note: The date you choose begins at 12 midnight.

4. Date to:—Click to access the Calendar.

   Choose the month and the year by using the arrows to scroll to the needed options.

   Choose the day by clicking the appropriate cell or by clicking Today.

Note: The date you choose ends at 11:59:59 PM.

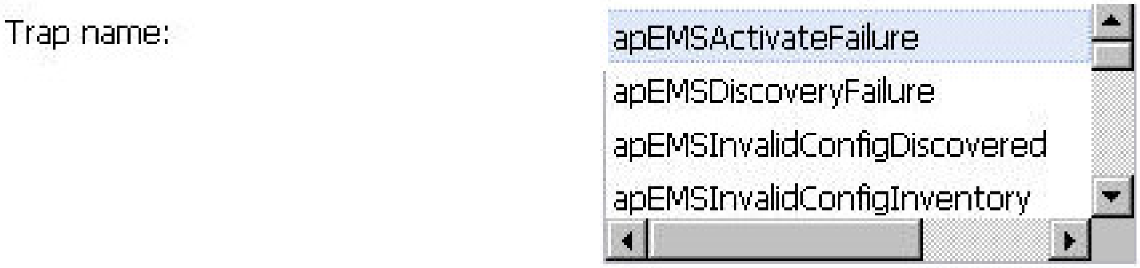
5. Source:—Enter the source name for this device.

Source device: 172.30.80.120

6. Source IP:—Enter the IP address for this source device.

Source IP: 172.30.80.120

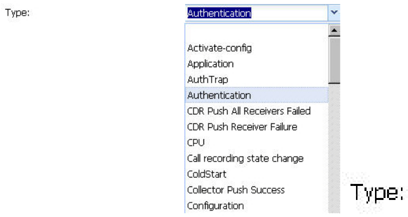
7. Trap name:—Choose the trap name from the list.



Trap name:

apEMSActivateFailure
apEMSDiscoveryFailure
apEMSInvalidConfigDiscovered
apEMSInvalidConfigInventory

8. Type:—Choose the type for this alarm from the drop-down list.

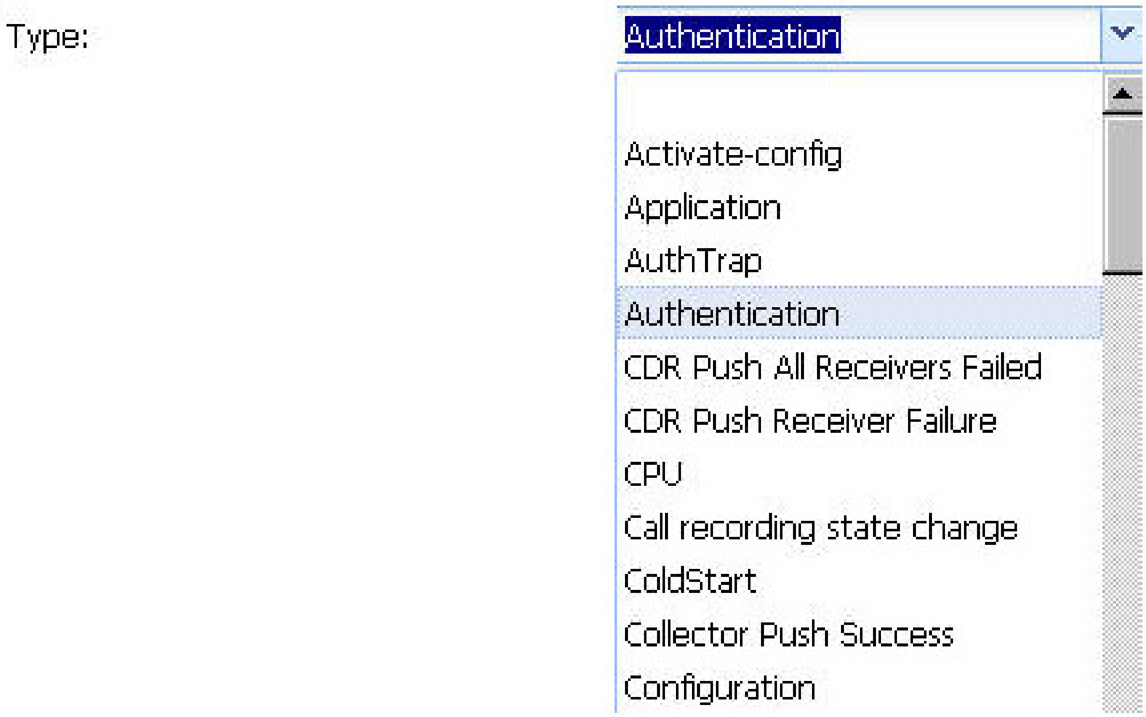


Type: Authentication

Activate-config
Application
AuthTrap
Authentication
CDR Push All Receivers Failed
CDR Push Receiver Failure
CPU
Call recording state change
ColdStart
Collector Push Success
Configuration

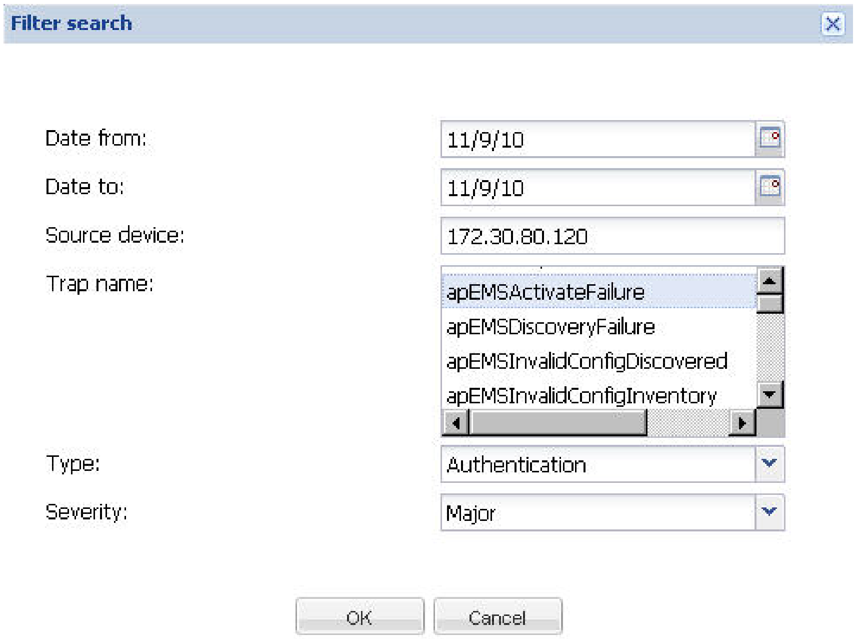
Type:

9. Severity:—Choose the severity level for this alarm from the drop-down list.



Type: Authentication

10. Click OK.



Filter search

Date from: 11/9/10

Date to: 11/9/10

Source device: 172.30.80.120

Trap name: apEMSActivateFailure

Type: Authentication

Severity: Major

11. Click Cancel to cancel the Filter search criteria.

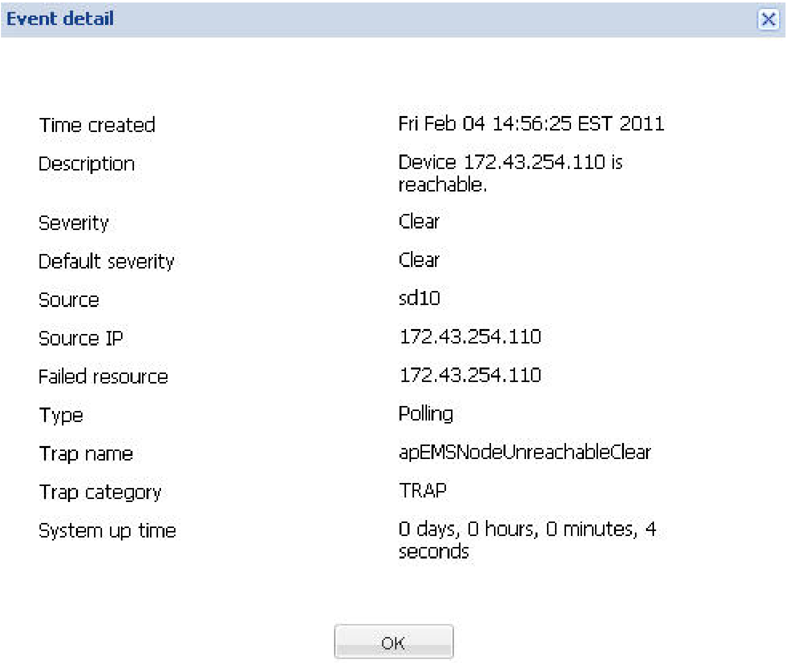
Viewing Event Details

You can access details about each event listed in the content area.

To view event details:

1. Expand the Fault Manager slider and click Events. The events data appears in the content area.
2. Click the event in the table for which you want to view event details and click View.
3. Click Show all to view all events.

The Event detail dialog box appears.



Event detail

Time created	Fri Feb 04 14:56:25 EST 2011
Description	Device 172.43.254.110 is reachable.
Severity	Clear
Default severity	Clear
Source	sd10
Source IP	172.43.254.110
Failed resource	172.43.254.110
Type	Polling
Trap name	apEMSNodeUnreachableClear
Trap category	TRAP
System up time	0 days, 0 hours, 0 minutes, 4 seconds

4. Click OK to close the dialog box.

   The following table describes the information found in the dialog box.

Event Category	Description
Time created	Date and time this event was generated
Description	Short description of the event
Severity	User-defined severity level for this event: Critical Major Minor Clear Warning Info
Default Severity	System-defined severity level for this event
Source	Exact source of the event
Source IP	Source IP address of the event
Failed resource	Resource responsible for the event
Type	Type of trap associated with this event
Trap Name	Exact name of the trap associated with this event
Trap Category	Category to which the event belongs
System up time	Length of time the system has been operational in hours, minutes, and seconds. See the System up time section below for further information.

System Up Time

The System up time field of the Event Detail dialog box can apply to either the device system up time, or the Oracle Communications Session Delivery Manager server system up time. If the event Type column is one of the following types below, then this field applies to Oracle Communications Session Delivery Manager server up time. Otherwise, this information pertains to the device system up time.

Event types pertaining to Oracle Communications Session Delivery Manager server system up time:

- Configuration
- Polling
- HealthMonitor

Saving Events Data

You can save the data displayed on each screen to a csv file in comma separated values format.

To save data to a file:

1. With the data displayed, click Save to file.

   A Save window opens with a file name, for example:

   ```
   events.csv
   ```
2. Click Save to file to save the data to a file and close the window.

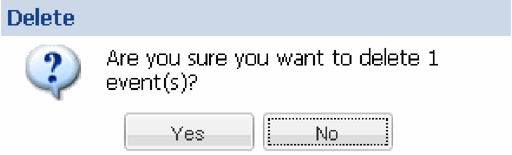
Deleting Events Data

With appropriate permissions assigned, you can delete events data in Oracle Communications Session Delivery Manager.

Note: Deleting an event has no affect on the Net-Net SBC. The Net-Net SBC is unaware that Oracle Communications Session Delivery Manager ever displayed the event, or deleted it.

To delete events data:

1. Click on the event you want to delete to select it.
2. Click Delete. A confirmation message appears.



Delete

Are you sure you want to delete 1 event(s)?

3. Click No to cancel this delete operation.
4. Click Yes to proceed with the deletion. An Info dialog box appears to confirm the event was deleted successfully.
5. Click OK to clear the message. The events table automatically refreshes with the event you deleted removed from the table.

Alarms

This section explains how to view information about alarms. Alarms play a significant role in determining overall health of the system. For additional information about alarms, see the Oracle MIB Reference Guide.

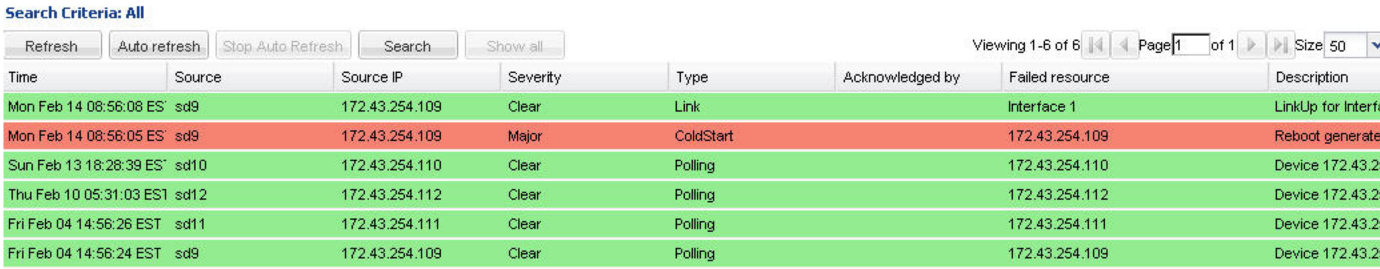
An alarm is triggered when a condition or event happens within either the Net-Net system’s hardware or software. Alarms contain an alarm code, a severity level, a textual description of the event, and the time the event occurred.

Displaying the Alarm View

The Alarm view displays the current list of alarms for devices.

To view alarm data:

Expand the Fault Manager slider and click Alarms. The list of current alarms appears in the content area.



Time	Source	Source IP	Severity	Type	Acknowledged by	Failed resource	Description
Mon Feb 14 08:56:08 ES	sd9	172.43.254.109	Clear	Link		Interface 1	LinkUp for Interf
Mon Feb 14 08:56:05 ES	sd9	172.43.254.109	Major	ColdStart		172.43.254.109	Reboot generate
Sun Feb 13 18:28:39 ES	sd10	172.43.254.110	Clear	Polling		172.43.254.110	Device 172.43.2
Thu Feb 10 05:31:03 ES	sd12	172.43.254.112	Clear	Polling		172.43.254.112	Device 172.43.2
Fri Feb 04 14:56:26 EST	sd11	172.43.254.111	Clear	Polling		172.43.254.111	Device 172.43.2
Fri Feb 04 14:56:24 EST	sd9	172.43.254.109	Clear	Polling		172.43.254.109	Device 172.43.2

Customizing the Alarms Table Display

The alarms are displayed in the order of precedence based on time and in descending order. You can customize the data presented in the alarms table by changing the columns that are displayed and/or the order of the table entries. To customize the table display, see *Customizing the Table Display*.

The following table describes the information displayed in the list of alarms.

Options	Description
Time	Date and time the alarm was generated in hours, minutes, and seconds
Source	Specific host name or IP address from which this alarm was generated
Source IP	Source IP address of the alarm
Severity	Current alarm severity level, for example, critical, major, minor
Type	Type of alarm, for example, coldstart, polling, health
Trap name	Exact name of the trap associated with this alarm
Acknowledged by	Whether an alarm has been acknowledged
Failed resource	Resource responsible for the alarm
Description	Textual description of the alarm
Source group ID	Source group ID associated with this alarm
Object ID	Object ID associated with this alarm

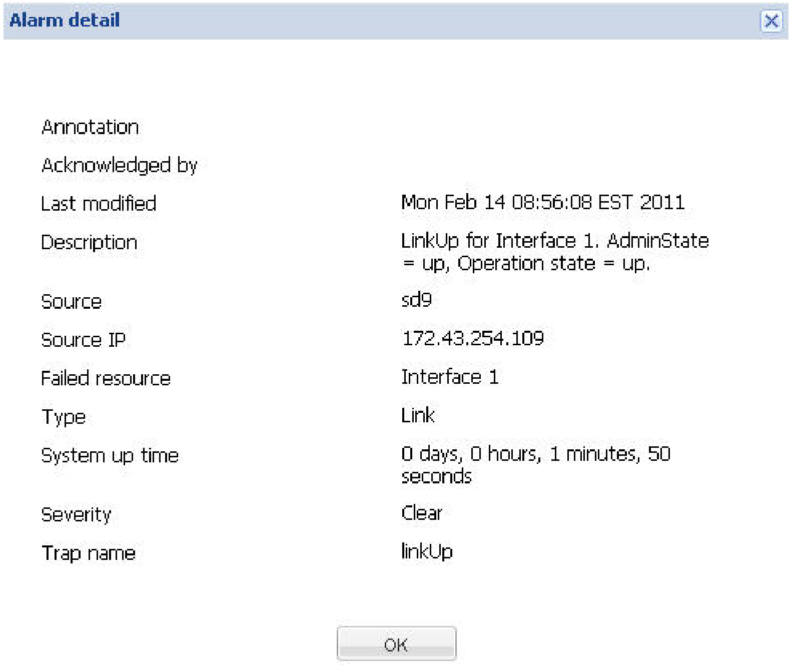
Alarm Details

You can view additional details about each alarm listed in the alarms table.

To view alarm details:

1. Expand the Fault Manager slider and click Alarms. The alarms data appears in the content area.
2. Click the alarm in the table for which you want to view event details and click View.

   The Alarm detail dialog box appears.



Alarm detail

Annotation	
Acknowledged by	
Last modified	Mon Feb 14 08:56:08 EST 2011
Description	LinkUp for Interface 1. AdminState = up, Operation state = up.
Source	sd9
Source IP	172.43.254.109
Failed resource	Interface 1
Type	Link
System up time	0 days, 0 hours, 1 minutes, 50 seconds
Severity	Clear
Trap name	linkUp

3. Click OK to close the dialog box.

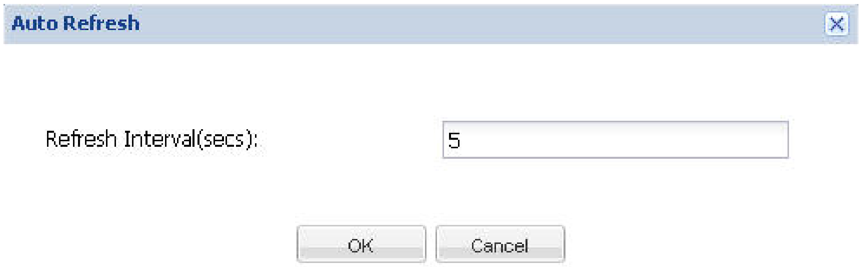
The following table describes the information displayed in the Alarm detail dialog box.

Options	Description
Annotation	A user-defined note pertaining to this alarm
Acknowledged by	User that acknowledged the alarm
Last modified	Date and time the alarm was last modified
Description	Generated by trap input associated with this alarm
Source	Source of the alarm
Source IP	Source IP address of this alarm
Failed resource	Failed resource that generated the alarm
Type	Type of alarm
System up time	Length of time the system has been operational in hours, minutes, and seconds
Severity	Current severity of alarm: Emergency Critical Major Minor Warning Clear
Trap name	Exact name of the trap associated with this alarm

Configuring Auto Refresh

To configure auto refresh for alarm data:

1. Expand the Fault Manager slider and click Alarms. The alarms data appears in the content area.
2. Click Auto refresh. The Auto Refresh dialog box appears.
3. Refresh Interval(secs):—Enter the number of seconds you want to configure for auto refresh.



Refresh Interval(secs): 5

4. Click OK or click Cancel to cancel auto refresh configuration.

Stopping Auto Refresh

When Auto refresh is configured, Stop Auto Refresh becomes enabled.

To stop auto refresh:

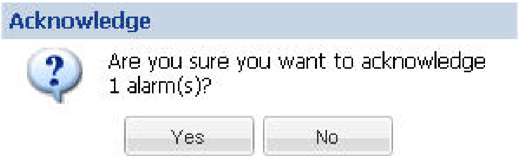
Click Stop Auto Refresh. Auto refresh is disabled.

Acknowledging Alarms

With the appropriate admin privileges assigned, you can acknowledge alarms. When you acknowledge an alarm the Acknowledged by and Last modified fields are updated.

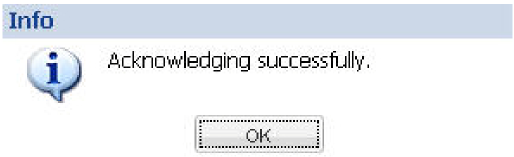
To acknowledge alarms:

1. Expand the Fault Manager slider and click Alarms. The alarms data appears in the content area.
2. Click the alarm you want to acknowledge in the alarms table and click Acknowledge. The Acknowledge dialog box appears.



Are you sure you want to acknowledge 1 alarm(s)?

3. Click Yes. An Info dialog box appears.



Acknowledging successfully.

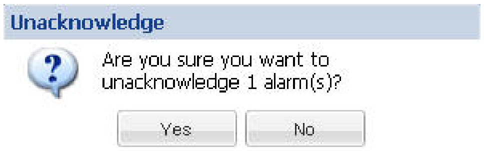
4. Click OK.
5. Click the alarm to view an updated Alarm detail screen with the Acknowledged by and Last modified fields updated.
6. Click OK.

Unacknowledging Alarms

With the appropriate admin privileges, you can unacknowledge alarms by clicking Unacknowledge on the Alarms window.

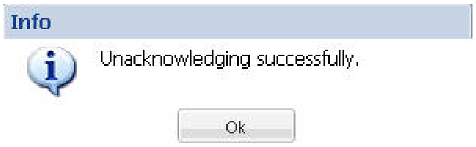
To unacknowledge alarms:

1. Click the alarm you want to unacknowledge and click Unacknowledge. The Unacknowledge dialog box appears.



Are you sure you want to unacknowledge 1 alarm(s)?

2. Click Yes. The Info dialog box appears.



Unacknowledging successfully.

3. Click OK.

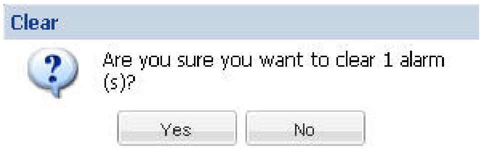
Clearing Alarms

With the appropriate admin privileges, you can clear alarms by clicking Clear on the Alarms window. Clearing an alarm changes the alarm's severity to clear.

Note: Clearing an alarm in Oracle Communications Session Delivery Manager has no affect on the Net-Net SBC. The Net-Net SBC is unaware that Oracle Communications Session Delivery Manager displayed the alarm, or changed it's severity to clear.

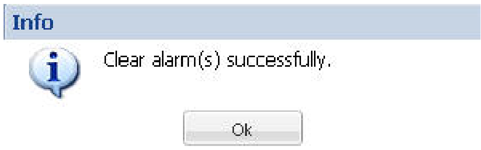
To clear alarms:

1. Expand the Fault Manager slider and click Alarms. The alarms data appears in the content area.
2. Click the alarm you want to clear and click Clear. The Clear dialog box appears.



Are you sure you want to clear 1 alarm (s)?

3. Click Yes. The Info dialog box appears.



Clear alarm(s) successfully.

4. Click Ok. The alarm severity changes to clear.

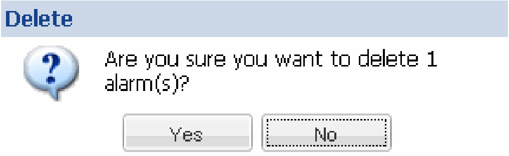
Deleting Alarms

With the appropriate admin privileges, you can delete alarms by clicking Delete on the Alarms window. Deleting an alarm removes the alarm from the alarms table. You are prompted to confirm deleting the alarm and the alarm is removed from the Oracle Communications Session Delivery Manager display and database for all Oracle Communications Session Delivery Manager users.

Note: Deleting an alarm in Oracle Communications Session Delivery Manager has no affect on the Net-Net SBC. The Net-Net SBC is unaware that Oracle Communications Session Delivery Manager displayed the alarm, or deleted it from the alarms table.

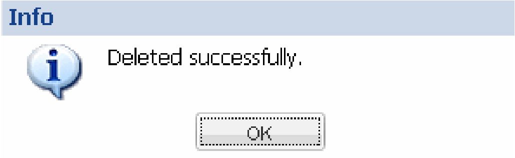
To delete alarms:

1. Expand the Fault Manager slider and click Alarms. The alarms data appears in the content area.
2. Click the alarm you want to clear and click Delete. The Delete dialog box appears.


Delete

Are you sure you want to delete 1 alarm(s)?

3. Click Yes. The Info dialog box appears.


Info

Deleted successfully.

4. Click OK. The alarm is deleted from the alarms table and database.

Alarm Actions

There are a set of actions you can perform from the alarms content area. Some of these actions require admin permissions assigned:

- Refresh: Refresh the data in the table
- Auto refresh: Customize the auto refresh interval in seconds
- Stop Auto refresh: Cancel customized auto refresh, if enabled
- Search: Perform a filtered search of alarms by: Date range, source IP, source type, and alarm severity
- Show all: Show all current alarms
- View: View alarm details
- Edit: Add an annotation to the alarm detail dialog box
- Save to file: Save the alarm details to a file
- Clear: Clear the alarm from the alarms table
- Acknowledge: Acknowledge an alarm
- Unacknowledge: Unacknowledge an alarm
- Delete: Delete the alarm from Oracle Communications Session Delivery Manager

Alarm Categories

The alarms displayed in the Oracle Communications Session Delivery Manager fall into the following categories:

Category	Description
apSysLog	Associated with the proprietary Oracle ap-slog.mib, which provides a method of gathering syslog messages generated by the Net-Net system via SNMP
apSysMgmt	Associated with the proprietary Oracle ap-smgmt.mi, which provides a means of gathering information about the status of the Net-Net system
ARP capacity	Percentage of ARP table in CAM utilization. Associated with the apSysMgmtGroup trap
AuthTrap	Associated with the standard authenticationFailure trap. The SNMPv2 agent received a protocol message that was not properly authenticated
ColdStart	Associated with the standard coldStart trap. The SNMPv2 agent is reinitializing itself and its configuration may have been altered
CPU	Percentage of CPU utilization. Associated with the apSysMgmtGroupTrap
Cpu load	CPU utilization percentage of application tasks has exceeded the threshold algd-load-limit
Discovery	Discovery status
DoS	Proprietary trap generated by Oracle Denial of Service protection

Category	Description
Gateway	Status of gateway reachability. Associated with the apSysMgmtGatewayUnreachableTrap trap
EMS-HA	Generated by the Oracle Communications Session Delivery Manager in a Oracle Communications Session Delivery Manager failover situation
Enhanced DoS	A device exceeded configured thresholds and was denied access by the Net-Net SBC
Fan	Fan unit speed fell below the monitoring level
H323 Stack	Status of H.323 stack. Associated with the apSysMgmtH323InitFail trap
HDR	Server specified becomes unreachable by the system collector
Health	System health percentage. Associated with the apSysMgmtGroupTrap
I2C	The Inter-IC bus (I2C) state changed from normal (1) to not functioning (7)
License	Associated with the proprietary Oracle ap-license.mib, which provides information about the status of your Net-Net licenses
Link	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	Bandwidth allocation failed at a percentage higher or equal to the system’s default threshold rat
Media ports	Port allocation failed at a percentage higher or equal to the system’s default threshold rate
Media realm	Status of media realm. Associated with the apSysMgmtMediaUnknownRealm trap
Memory	Percentage of memory utilization. Associated with the apSysMgmtGroup trap
Monitor	Associated with the proprietary Oracle ap-env-monitor.mib, which gathers information about fan speed, voltage, temperature, and power supply for the Net-Net system. It also sends out traps when status changes occur
NAT capacity	Percentage of NAT table (in CAM) utilization
NTP Clock Skew	NTP had to adjust the clock by more than 1000 seconds
NTP server	Specified NTP server became unreachable
NTP service	All configured NTP servers are unreachable
Polling	Generated by the Oracle Communications Session Delivery Manager to indicate ability to reach the Net-Net SBC
Power	Status of power supply. Associated with the apEnvMonStatusChangeNotification trap
Realm Minutes Exceeded	Monthly minutes exceeded for a realm
RADIUS Servers	Status of RADIUS server
Reboot	Proprietary version of the standard coldStart trap
Redundancy	State change occurred on either the primary or secondary system in a redundant (HA) pair
Save-config	Error occurred while the system was trying to save the configuration to memory

Category	Description
Session agent	Session agent information that includes hostname, IP address, status, and the reason for the status. Associated with the apSysMgmtStatusChange trap
Single unit redundancy	Status of a slot changed. The varbinds contain the new information for the slot
Surrogate registration	Status of surrogate registration. Associated with the apSysMgmtSurrogateRegFailed trap
Task	Indication of a suspended task. Associated with the apSysMgmtTaskSuspendTrap
Temperature	System temperature. Associated with the apSysMgmtTempTrap trap

Alarm Severities

The following table lists the alarm severities.

Alarm Severity	Description
Critical	Requires attention as soon as it is noted. If you do not attend to this condition immediately, there may be physical, permanent, and irreparable damage to your Net-Net system
Major	Functionality has been seriously compromised. As a result, this situation might cause loss of functionality, hanging applications, and dropped packets. If you do not attend to this situation, your Net-Net system will suffer no physical harm, but it will cease to function
Minor	Functionality has been impaired to a certain degree. As a result, you might experience compromised functionality. There will be no physical harm to your Net-Net system. However, you should attend to this type of alarm as soon as possible in order to keep your Net-Net system operating properly
Warning	Some irregularities in performance. This condition describes situations that are noteworthy, however, you should attend to this condition in order to keep your Net-Net system operating properly. For example, this type of alarm might indicate the Net-Net system is running low on bandwidth and you may need to contact your Oracle customer support representative to arrange for an upgrade
Clear	Alarm is cleared.

Default Alarm Severity Color Codes

The severity levels for the alarms are color coded with the following defaults. You can change the defaults, see *Alarm Severity Color-Coding*.

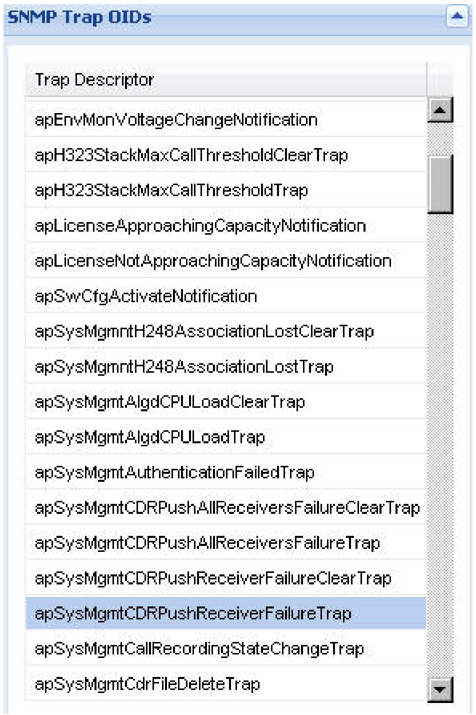
Alarm Severity	Default Alarm Severity Color
Critical	Red
Major	Salmon
Minor	Orange
Notice	Yellow
Warning	Light yellow
Info	Green yellow
Clear	Light green
All others	Lime

Remapping Alarm Severities

You can override the default severity levels for alarms.

To remap alarm severities:

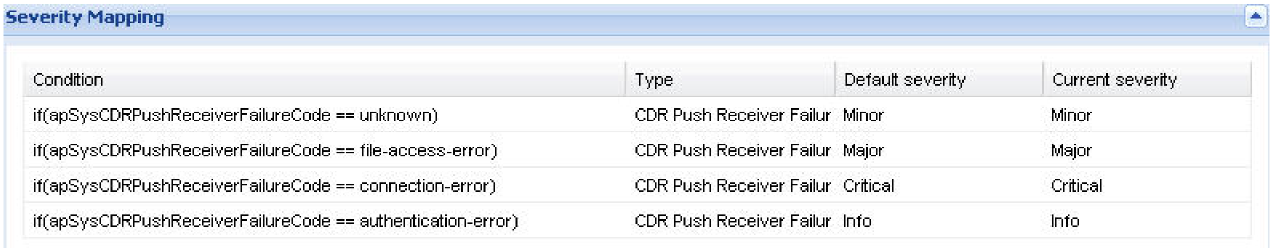
1. Expand the Fault Manager slider and click Trap event setting. The Trap Event Mapping appears in the content area.
2. Under SNMP Trap OIDs, click the Trap Descriptor name whose alarm severity you want to remap.



SNMP Trap OIDs

Trap Descriptor
apEnvMonVoltageChangeNotification
apH323StackMaxCallThresholdClearTrap
apH323StackMaxCallThresholdTrap
apLicenseApproachingCapacityNotification
apLicenseNotApproachingCapacityNotification
apSwCfgActivateNotification
apSysMgmntH248AssociationLostClearTrap
apSysMgmntH248AssociationLostTrap
apSysMgmtAlgdCPULoadClearTrap
apSysMgmtAlgdCPULoadTrap
apSysMgmtAuthenticationFailedTrap
apSysMgmtCDRPushAllReceiversFailureClearTrap
apSysMgmtCDRPushAllReceiversFailureTrap
apSysMgmtCDRPushReceiverFailureClearTrap
apSysMgmtCDRPushReceiverFailureTrap
apSysMgmtCallRecordingStateChangeTrap
apSysMgmtCdrFileDeleteTrap

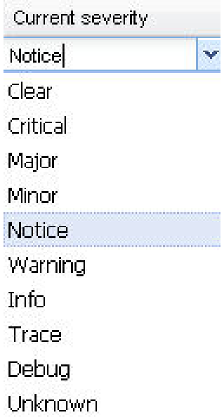
The information for that condition appears in Severity Mapping table below.



Severity Mapping

Condition	Type	Default severity	Current severity
if(apSysCDRPushReceiverFailureCode == unknown)	CDR Push Receiver Failur	Minor	Minor
if(apSysCDRPushReceiverFailureCode == file-access-error)	CDR Push Receiver Failur	Major	Major
if(apSysCDRPushReceiverFailureCode == connection-error)	CDR Push Receiver Failur	Critical	Critical
if(apSysCDRPushReceiverFailureCode == authentication-error)	CDR Push Receiver Failur	Info	Info

3. Click the row of the condition you want to modify in the Current severity column. A drop-down list of severity levels appears.



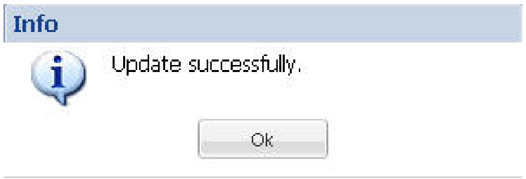
Current severity

Notice

Clear
Critical
Major
Minor
Notice
Warning
Info
Trace
Debug
Unknown

4. Click the severity you want to apply in the drop-down list to select it. The new level appears in the Current Severity column.

   The Default severity column will still retain the default severity for this condition.
5. Click Apply. The Info dialog box appears.



Info

Update successfully.

6. Click Ok.
7. Repeat steps 2 through 7 for each condition you want to remap current severity for.

   The new value will apply to all subsequent client displays.

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 application.

Alarm Frequency

The alarm will replay at a frequency set in the Audible Alarms configuration. For example, a frequency of 5 will sound the alarm sound every 5 seconds. Setting the frequency to 0 results in the alarm sound playing once.

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 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 an Audible Alarm

You must configure Audible Alarms in Net-Net Central before launching it from the Fault Manager application..

To configure audible alarms:

1. Click Settings in the Net-Net Central menu bar. A drop-down menu appears.
2. Click **Alarms** > **Audible Alarms**.
3. Click the **Enable audio alarm** check box of each severity you want to enable.
4. **Frequency**— Click the number to edit the audible alarm frequency. This value is entered in seconds. The default is 5.
5. Click **OK**.

To launch the Audible Alarms application:

6. Expand the Fault Manager slider and click Alarms.
   The Alarms table appears in the content area.
7. Click **Auto Refresh**.

8. **Refresh interval (secs)**— Enter a value in seconds for how often the Alarms table is automatically refreshed.
9. Click **OK**.
10. Click **Start Audible Alarms**.
    The button toggles to Stop Audible Alarms.

To shut down the Audible Alarms application:

11. Expand the Fault Manager slider and click Alarms.
    The Alarms table appears in the content area.
12. Click **Stop Audible Alarms**.
    The button toggles to Start Audible Alarms.

Selecting Alarm Criteria

You can filter selected alarms to choose the ones you want to save or delete. You can select alarms using one, some, or all of the selection criteria. For example, you can select alarms for a specific IP address during a specified date-time range.

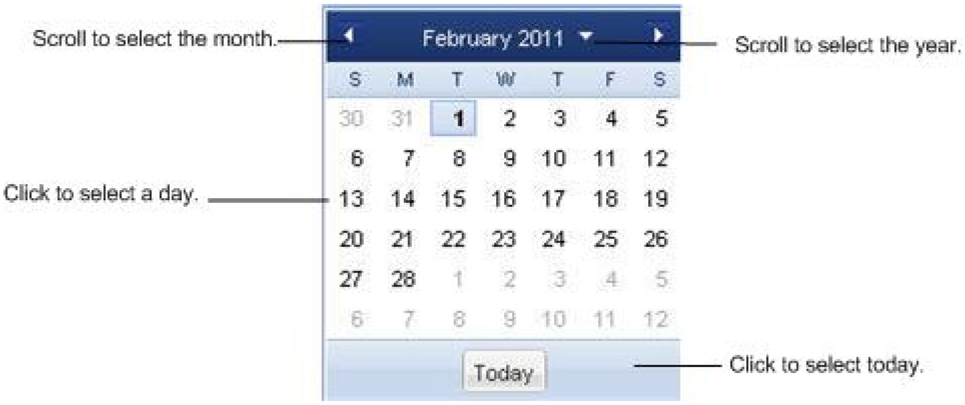
Configuring Alarm Selection

To configure alarm selection:

1. Expand the Fault Manager slider and click Alarms. The alarms table appears in the content area.
2. Click Search. The Filter search dialog box appears.
3. Date from:—Click 📅 to access the Calendar.

   Choose the month and the year by using the arrows to scroll to the needed options.

   Choose the day by clicking the appropriate cell or by clicking Today.



S	M	T	W	T	F	S
30	31	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	1	2	3	4	5
6	7	8	9	10	11	12

Note: The date you choose begins at 12 midnight.

4. Date to:—Click 📅 to access the Calendar.

   Choose the month and the year by using the arrows to scroll to the needed options.

   Choose the day by clicking the appropriate cell or by clicking Today.

   Note: The date you choose ends at 11:59:59 PM.

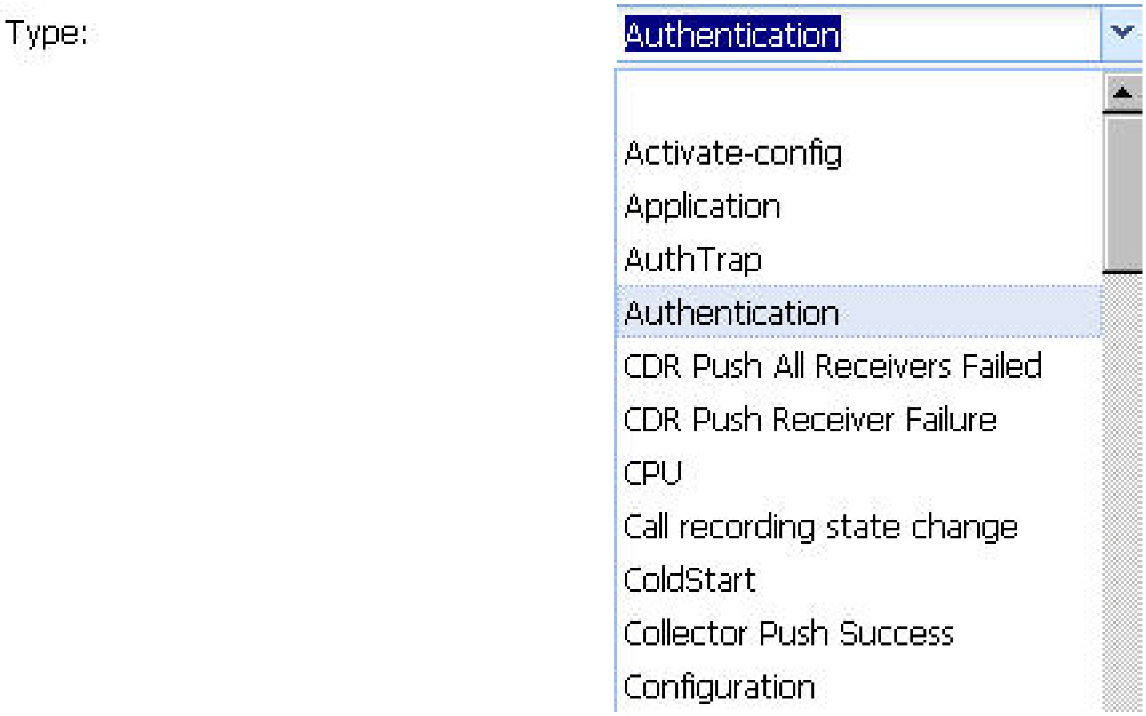
5. Source:—Enter the name of this source device.

Source device: 172.30.80.120

6. Source IP:—Enter the IP address for this source device.

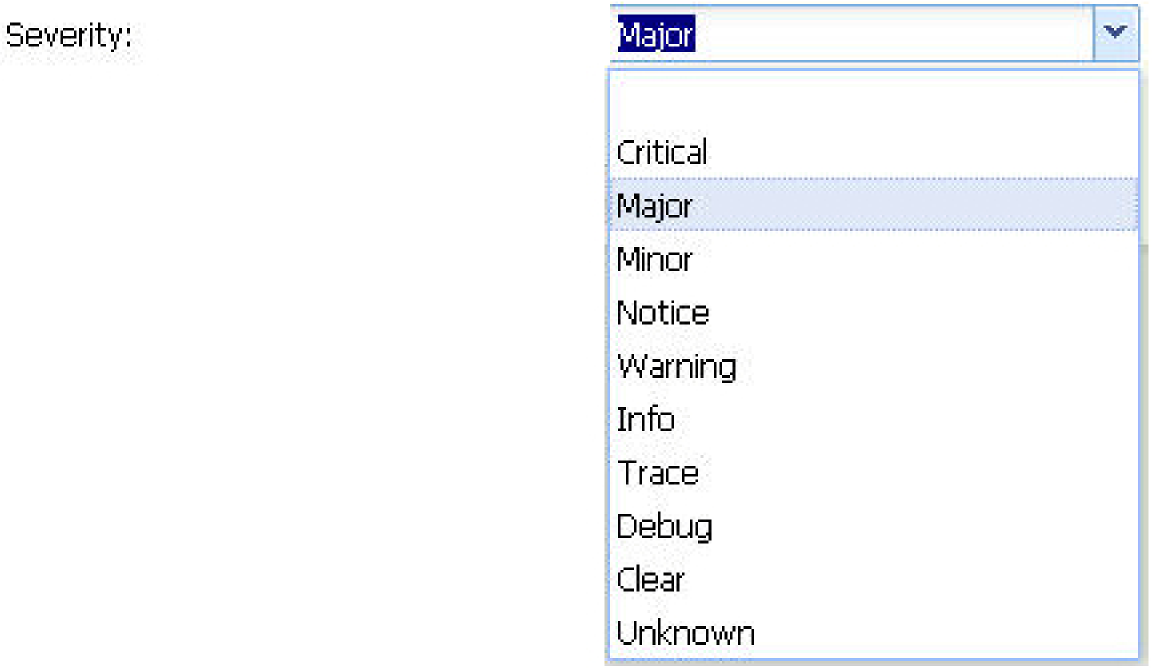
Source IP: 172.43.245.112

7. Type:—Choose the type for this alarm from the list.



Type: Authentication

8. Severity:—Choose the severity level for this alarm from the drop-down list.



Severity: Major

9. Click OK.

10. Click Cancel to cancel the filter search criteria.

Saving Alarms Data

You can save the data displayed on each screen to a csv file.

To save data to a file:

1. With the data displayed, click Save to file.

   A Save window opens with a file name, for example:

```
alarms.csv
```

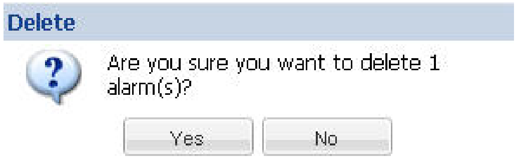
2. Depending on your browser, you will have an option to view this file or to save it.

   Click OK to save the file and close the window.

Deleting Alarms

To delete alarms:

1. Click the alarm you want to delete in the Alarms table.
2. Click Delete. A Delete message appears.


Delete

Are you sure you want to delete 1 alarm(s)?

3. Click Yes to proceed with the deletion
4. Click No to cancel the delete process.

   The alarm you selected for deletion is removed from the Alarms display.

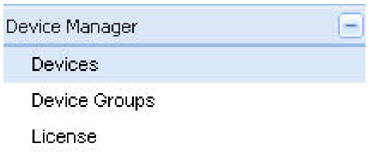
Synchronizing Alarms

If you have administrator privileges, you can synchronize the alarms displayed by Oracle Communications Session Delivery Manager with those maintained on those Net-Net SBCs that support alarm synchronization.

Triggering Alarm Synchronization

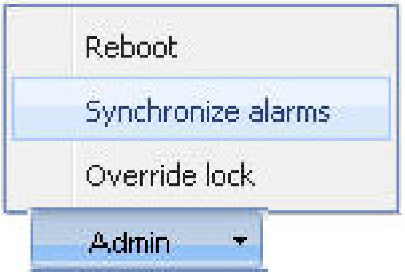
To trigger alarm synchronization for a device:

1. Expand the Device Manager slider and click Devices.

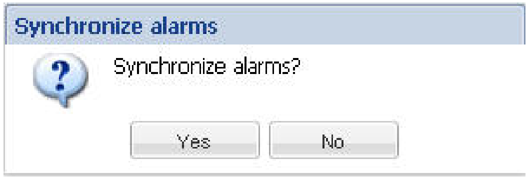


   The devices table appears in the content area.

2. Click the device you want to trigger alarm synchronization for and click Admin. A pop-up menu appears.
3. Click Synchronize alarms.



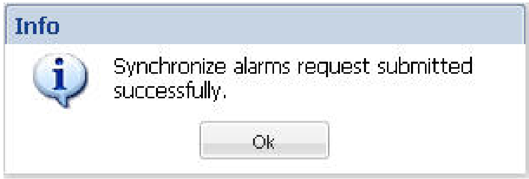
   The Synchronize alarms dialog box appears.



Synchronize alarms

Synchronize alarms?

4. Click Yes. The Info dialog box appears.



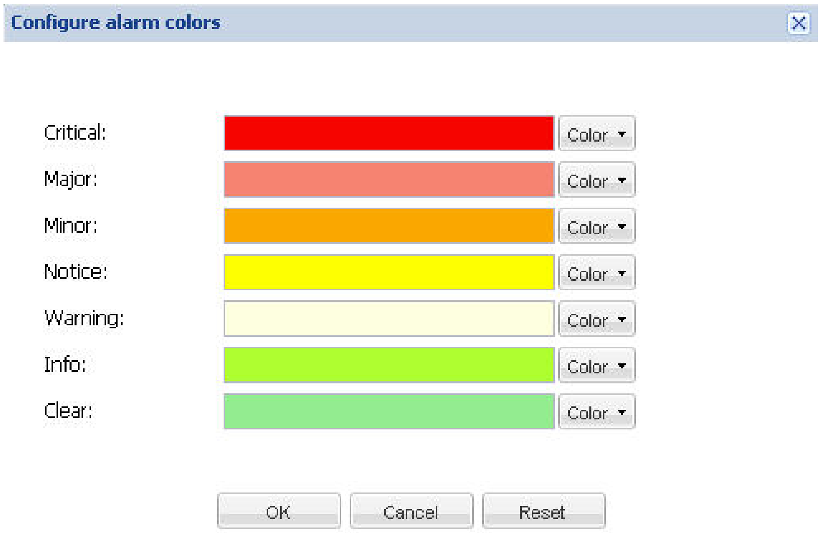
Info

Synchronize alarms request submitted successfully.

5. Click Ok.
6. To trigger alarm synchronization for additional devices, repeat steps 2 through 5.

Alarm Severity Color-Coding

You can configure the colors used to indicate the different severity levels. The system-default colors are shown in the image below:



Configure alarm colors

Critical:

Major:

Minor:

Notice:

Warning:

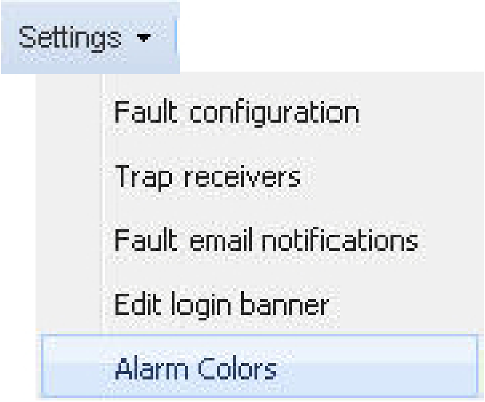
Info:

Clear:

Configuring Severity Color Coding

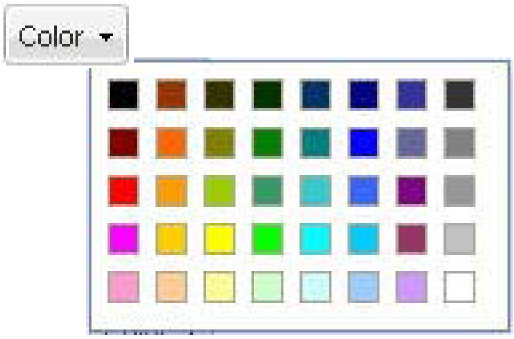
To configure alarm severity color coding:

1. Click Settings in the Oracle Communications Session Delivery Manager menu bar. A drop-down menu appears.
2. Click Alarm Colors.



The Configure alarm colors dialog box appears:

3. Click the arrow next to Color to open a color palette.



4. Click the color in the color palette you want to assign for each severity level.
5. Click OK. An Info dialog box confirms colors are successfully updated.
6. Click OK.

Note: Your new alarm color will not automatically update in the alarms table. To view your new alarm color, you must move to another tab, or another slider in the navigation pane, and then return to the alarms table to view the updated alarm color.

Clearing Events and Alarms Databases

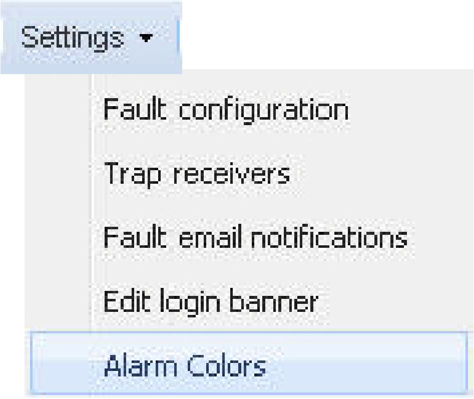
You can configure time frames to delete events and alarms data.

The default time frame for event data purge is seven days and the default time frame for alarm data purge is 14 days. However, when the *Clear events after (days) or the *Clear alarms after (days) parameters are set to 0, the event and alarm data remain in the databases and is not deleted.

Configuring Data Deletion Time Frames

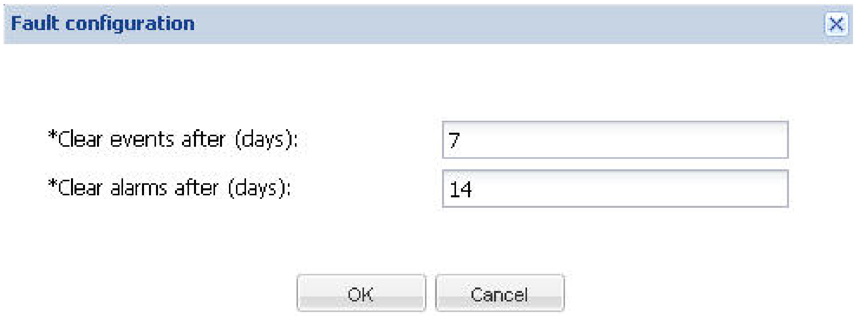
To configure time frames to delete events and alarms:

1. Click Settings in the Oracle Communications Session Delivery Manager menu bar. A drop-down menu appears.
2. Click Fault configuration.



The Fault configuration dialog box appears.

3. *Clear events after (days):—Enter the number of days you want to retain events in the database before the information is deleted. The default is 7 days.
4. *Clear alarms after (days):—Enter the number of days you want to retain alarms in the database before the information is deleted. the default is fourteen days.


Fault configuration

*Clear events after (days): 7

*Clear alarms after (days): 14

5. Click OK. The Info dialog box appears.
6. Click OK.

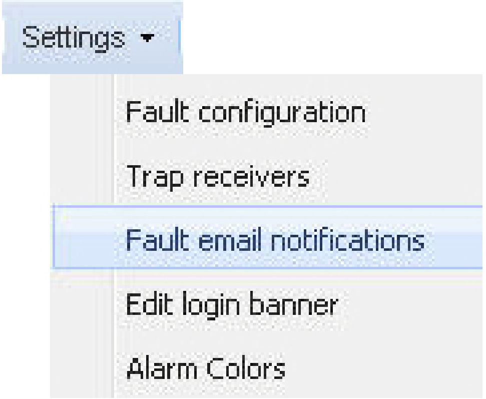
Fault Email Notifications

Oracle Communications Session Delivery Manager can trigger automatic email notifications when reporting alarms for certain severities. With the appropriate administrator privileges assigned, you can configure fault email addresses for each severity.

Configuring Fault Email Notifications

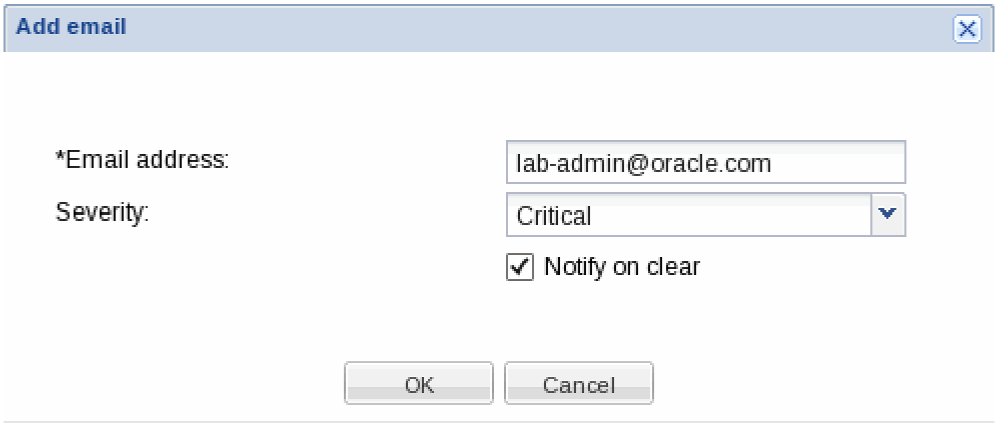
To configure a fault email list:

1. Click **Settings** in the top tool bar. A drop-down menu appears.
2. Click **Fault email notifications**.



The Fault email recipients dialog box appears.

3. Click **Add**. The Add email dialog box appears.
4. ***Email address:**—Enter the recipient's email address you want to attach to the alarm severity.
5. **Severity**—Click the severity from the drop-down list that you want to set for this email notification.


Add email

*Email address: lab-admin@oracle.com

Severity: Critical

☑ Notify on clear

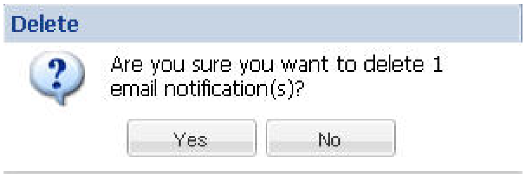
6. **Notify on clear**—Select the checkbox in order to send a fault notification on all clear events.
7. Click **OK**. The Info dialog box appears.
8. Click **OK**. Your entry is added to the Fault email recipients list.
9. Repeat steps 3 through 7 to add additional email notifications.
10. Click **Refresh** to refresh the data in the list.
11. Click **OK**.

Deleting Fault Email Notifications

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

To delete an email notification from the fault email recipients list:

1. Click Settings in the top tool bar. A drop-down menu appears.
2. Click Fault email notifications. The Fault email recipients dialog box appears.
3. Click the email address you want to delete and click Delete. The Delete dialog box appears.


Delete

Are you sure you want to delete 1 email notification(s)?

4. Click Yes. The Info dialog box appears.

5. Click OK. The email address is removed from the Fault email recipients list.
6. Repeat steps 3 through 5 to delete additional email notifications.
7. Click OK.

Editing Fault Email Notifications

With the appropriate administrator privileges assigned, you can edit fault email notifications for each severity.

To edit a fault email notification:

1. Click Settings in the top tool bar. A drop-down menu appears.
2. Click Fault email notifications. The Fault email recipients dialog box appears.
3. Click the email address you want to edit and click Edit. The Edit email dialog box appears.
4. *Email address:—Enter your changes in the text field, if any.
5. Severity—Click the severity you want to change in the drop-down list.
6. Click OK. The Info dialog box appears.
7. Click OK. The updated email notification appears in the Fault email recipients list.
8. Repeat steps 3 through 7 to edit additional email notifications.

Configuring External Trap Receivers

This section describes the Oracle Communications Session Delivery Manager traps contained in the Oracle Oracle Communications Session Delivery Manager MIB and the configuration of external trap receivers. Oracle Communications Session Delivery Manager generates traps when it detects the following:

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

You need to configure an external server as the receiver for these traps.

About Oracle Communications Session Delivery Manager Traps

Oracle Communications Session Delivery Manager generates the following traps.

Trap	Description
apEMSSaveFailNotification	Generated when Oracle Communications Session Delivery 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 Delivery Manager GUI for the save/activate, save, or offline save operations. The trap contains the Net-Net SBC node ID, the start and stop time of the save configuration attempt, and the user initiating the save operation.
apEMSActivateFailNotification	Generated when Oracle Communications Session Delivery Manager fails to activate a configuration, whether initiated from the SOAP XML API or the Oracle Communications Session Delivery Manager GUI for the save/activate or activate operations
apEMSNodeUnreachableNotifcation	Generated when a node's status changes from reachable to unreachable. The trap contains the Net-Net SBC's node ID and the time of the event.

Trap	Description
apEMSNodeUnreachableClearNotification	Clearing condition trap. Generated when a node's status changes from unreachable to reachable. The trap contains the Net-Net SBC's node ID and the time of the event.

Notification Objects

The Oracle Oracle Communications Session Delivery Manager MIB also lists the following notification objects, the information for which is contained in the generated traps.

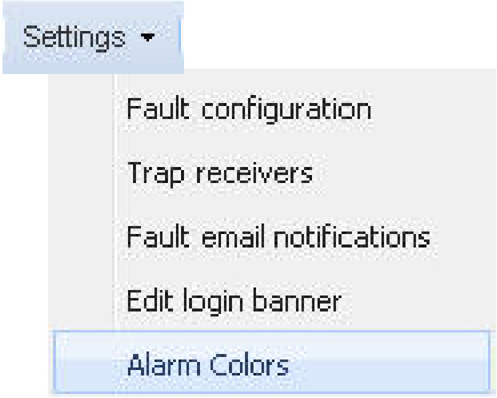
Notification Objects	Description
apEMSNodeID	Identifier for a Oracle Communications Session Delivery Manager node that appears on the navigation tree in the Active configuration area on the Discovery table in the Host Name/IP Address column
apCentralStartTime	Time as configured on the Oracle Communications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

Configuring External Trap Receivers

An external trap receiver is a server that you use as the trap destination, instead of the server where Oracle Communications Session Delivery 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.

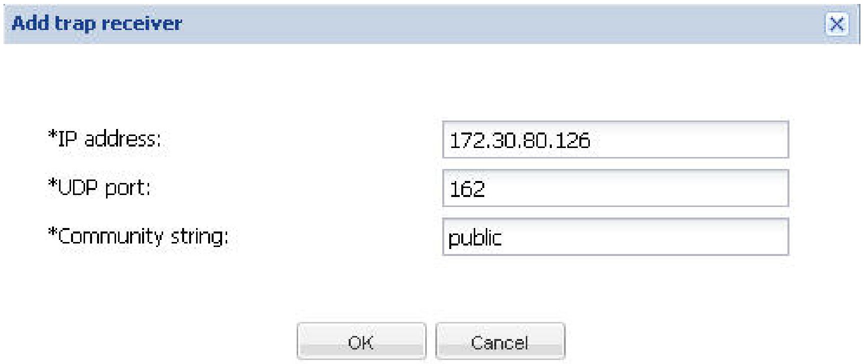
To configure external trap receivers:

1. Click Settings in the top tool bar. A drop-down menu appears.
2. Click Trap receivers.



   The Trap receivers configuration dialog box appears.
3. Click Add. The Add trap receiver dialog box appears.
4. *IP address:—Enter the IP address of the server receiving the traps.
5. *UPD port:—Enter the port number for the server receiving the traps or retain the default value of 162.

6. *Community string:—Enter the name of the SNMP community to which the server receiving traps belongs or retain the default value public.

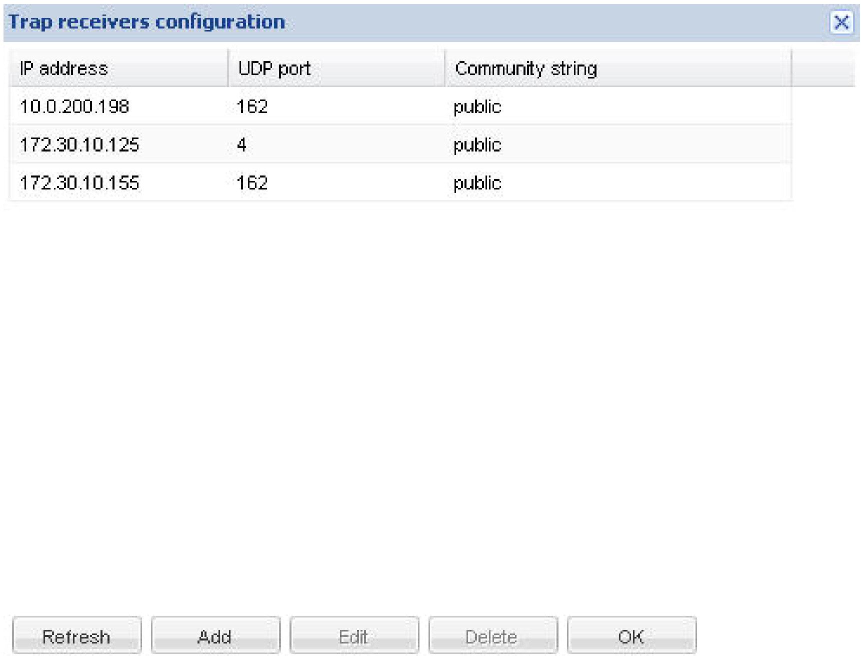


*IP address: 172.30.80.126

*UDP port: 162

*Community string: public

7. Click OK. An Info dialog box appears.
8. Click OK.



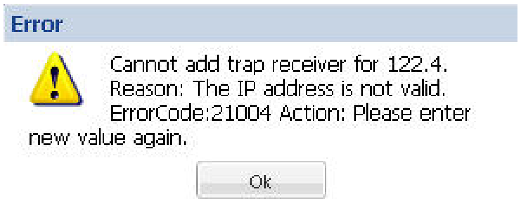
IP address	UDP port	Community string
10.0.200.198	162	public
172.30.10.125	4	public
172.30.10.155	162	public

The new trap is added to the Trap receivers configuration table.

Reporting Errors While Configuring Trap Receivers

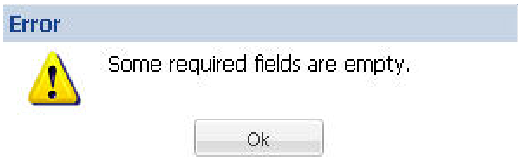
When configuring trap receivers, validations are performed on the IP address, port, and the community name you enter. If the IP address is entered in error, or if fields are left blank, the following error messages will appear:

- Incorrect IP address



Cannot add trap receiver for 122.4. Reason: The IP address is not valid. ErrorCode:21004 Action: Please enter new value again.

- Fields left empty



Some required fields are empty.

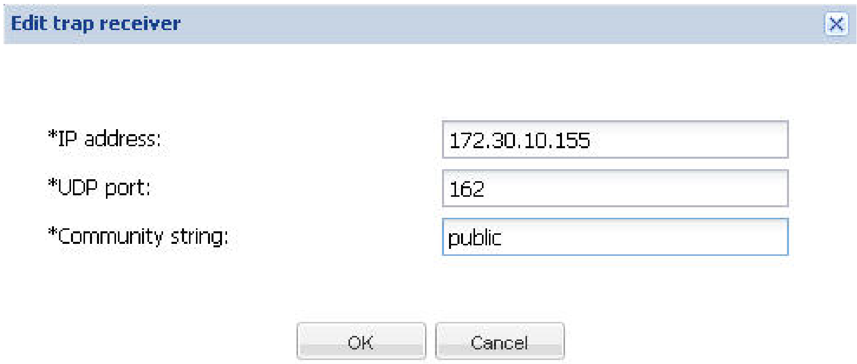
If necessary, click Ok to clear the error message.

Editing External Trap Receivers

You can edit an existing trap receiver to change its SNMP community name and state, destination address and port.

To edit an external trap receiver:

1. Click Settings in the top tool bar. A drop-down menu appears.
2. Click Trap receivers. The Trap receivers configuration dialog box appears.
3. Click the trap you want to edit in the Trap receivers configuration table and click Edit. The Edit trap receiver dialog box appears.



*IP address: 172.30.10.155

*UDP port: 162

*Community string: public

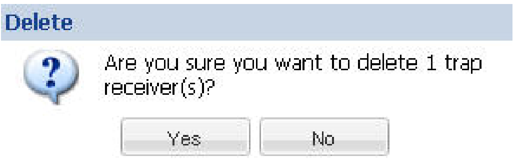
4. Edit the IP address, UDP port, and/or the Community name.
5. Click OK. The Info dialog box appears.
6. Click OK.

Deleting External Trap Receivers

You can delete traps from the Trap receivers configuration table.

To delete an external trap receiver:

1. Click Settings in the top tool bar. A drop-down menu appears.
2. Click Trap receivers. The Trap receivers configuration dialog box appears.
3. Click the trap you want to delete in the Trap receivers configuration table and click Delete. The Delete dialog box appears.



Are you sure you want to delete 1 trap receiver(s)?

4. Click Yes. The Info dialog box appears.
5. Click OK.

6

Viewing Performance Information

Overview

Performance Manager monitors your Net-Net SBCs by collecting necessary data from each of them. The performance measured is based on various factors, such as number of bytes of data received/sent (over a period) by a particular interface of a device, the interface's current bandwidth in bits-per-second, and so on.

Oracle Communications Session Delivery Manager displays the statistical and state information provided by the Net-Net SBC software (in the form of MIBs).

In Oracle Communications Session Delivery Manager, performance manager statistics are gathered for display on-demand when you access a Performance Manager screen or when you click the Refresh button. To preserve data, you must save it to a file by using the Save to file button.

☞ **Note:** You need to configure the SNMP community parameter on the Net-Net SBCs for which you want to view performance data. See the Oracle Communications Session Delivery Manager Configuration Guide and the Net-Net ACLI Reference Guide for details.

Accessing Performance Manager

This section explains how to access the Net-Net SBC performance information displayed by Oracle Communications Session Delivery Manager. Listed under Performance Manager in the navigation pane is a set performance groups containing information for your managed devices.

C-Series Performance Data

The following information is listed for C-series Net-Net SBCs:

- System
- SNMP
- IP
- Environmental
- Realms
- SIP session
- H323 session
- NSEP
- Trap table summary

- Storage utilization
- IDS
- Cached contacts
- NM controls
- ENUM servers

D-Series Performance Data

The following information is listed for D-series Net-Net SBCs:

- System
- SNMP
- IP
- Environmental
- Realms
- SIP session
- H323 session
- Codec
- Transcoding
- Cached contacts
- NM controls
- ENUM servers
- CPU core table

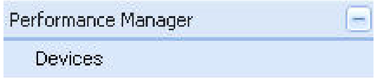
Note: In the performance manager table, each device in a cluster is listed individually. You can view performance data for each device in the cluster.

Selecting Managed Devices

You can view performance data for a specific device by first clicking Devices and then choosing the device. And then choosing the performance data category, for example, SNMP. You will retrieve SNMP performance data only for the device you selected.

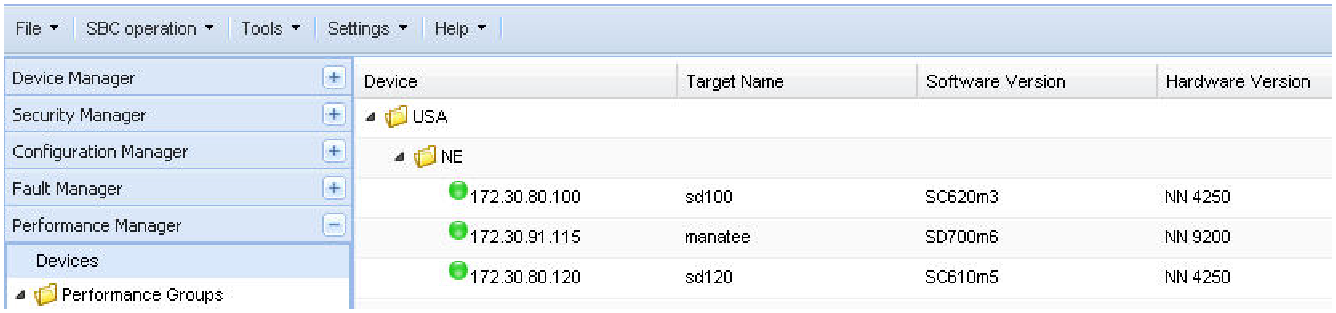
To select a device:

1. Click the plus (+) sign next to Performance manager. Devices appears.



2. Click Devices. The Device window appears in the content area.
3. Click the device folder to display all devices within this group.

The devices are the Net-Net SBCs managed by Oracle Communications Session Delivery Manager and for which you can view performance statistics. For example:

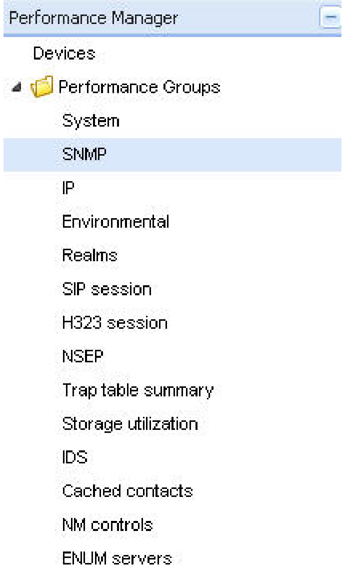


Device	Target Name	Software Version	Hardware Version
USA			
NE			
172.30.80.100	sd100	SC620m3	NN 4250
172.30.91.115	manatee	SD700m6	NN 9200
172.30.80.120	sd120	SC610m5	NN 4250

The following data is displayed for each device in the device content area:

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

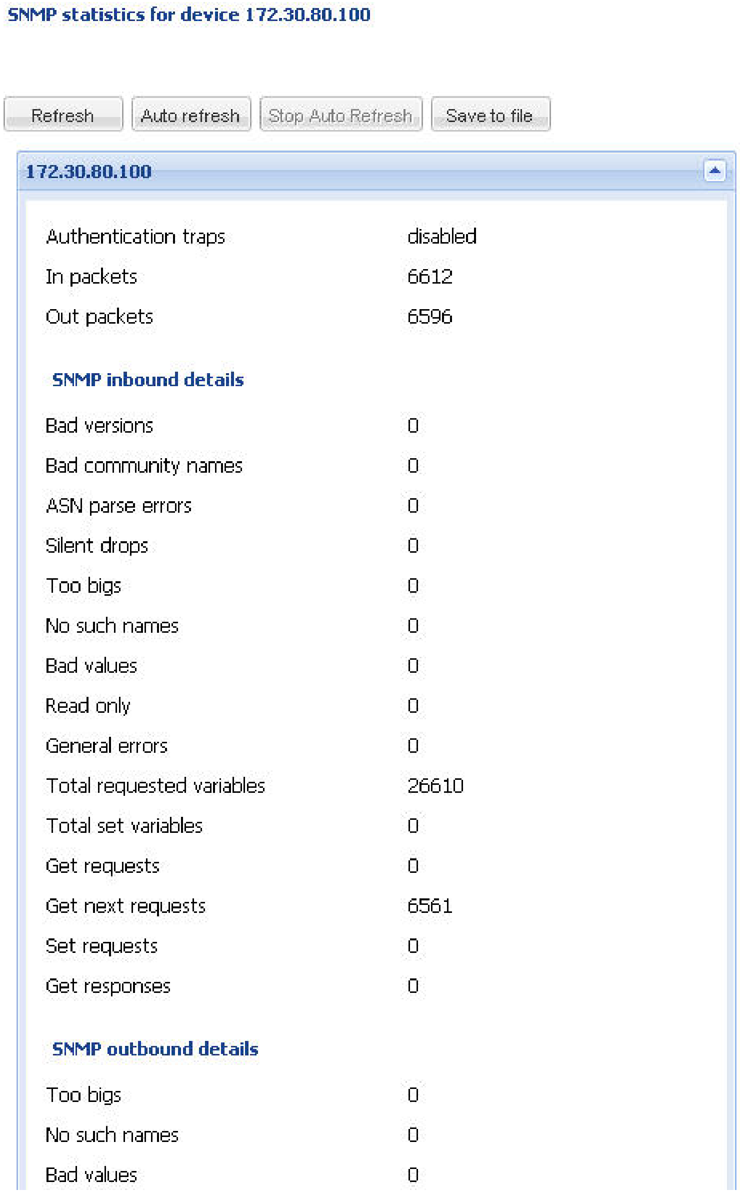
4. Click the device you want to view performance data for and click View (or double-click on the device). The performance groups folder expands to include a list of performance categories.
5. Click the performance category you want to view, for example SNMP.



Performance Manager

- Devices
- Performance Groups
  - System
  - SNMP
  - IP
  - Environmental
  - Realms
  - SIP session
  - H323 session
  - NSEP
  - Trap table summary
  - Storage utilization
  - IDS
  - Cached contacts
  - NM controls
  - ENUM servers

The SNMP data appears in the content area.



SNMP statistics for device 172.30.80.100

172.30.80.100

Authentication traps	disabled
In packets	6612
Out packets	6596

SNMP inbound details

Bad versions	0
Bad community names	0
ASN parse errors	0
Silent drops	0
Too bigs	0
No such names	0
Bad values	0
Read only	0
General errors	0
Total requested variables	26610
Total set variables	0
Get requests	0
Get next requests	6561
Set requests	0
Get responses	0

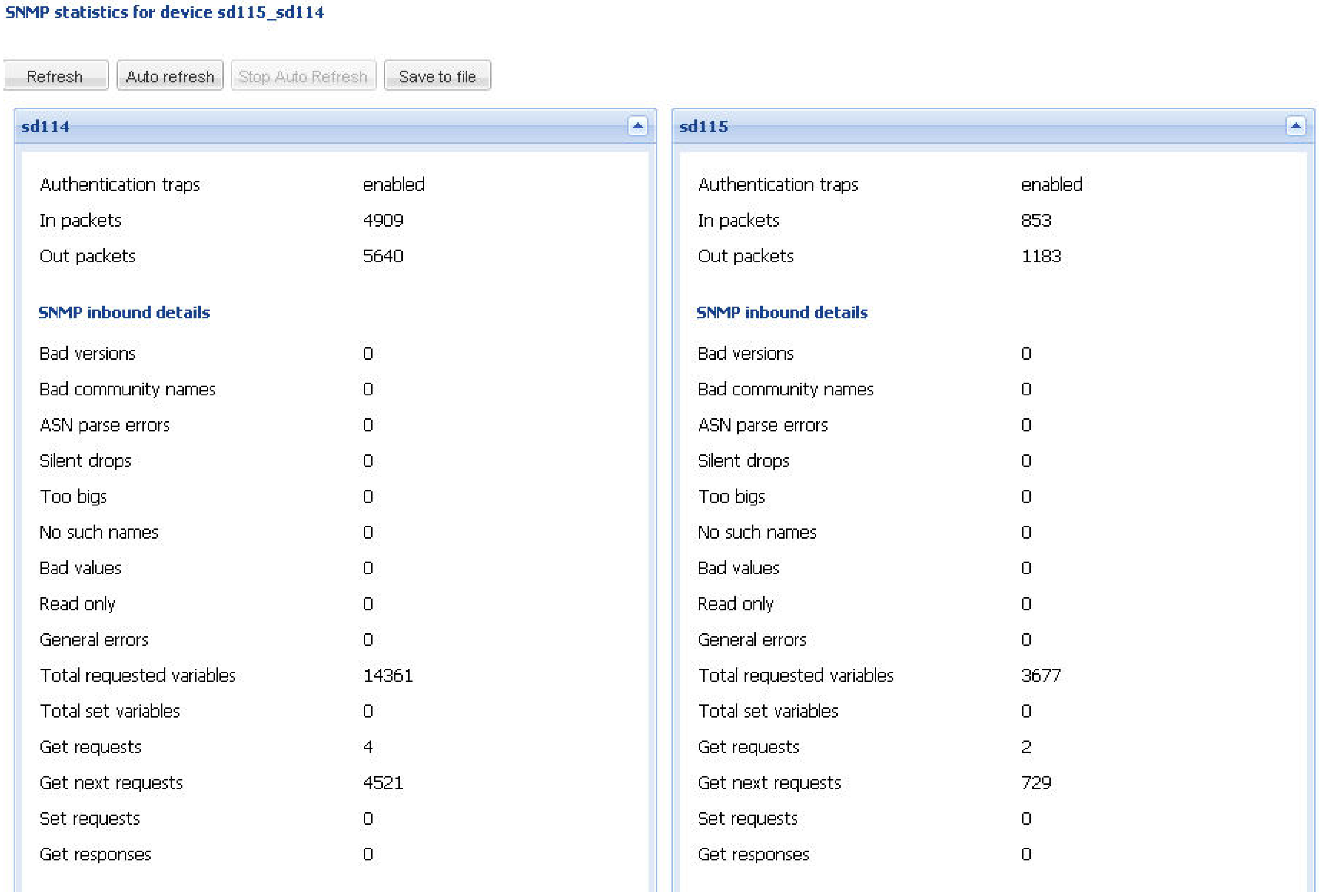
SNMP outbound details

Too bigs	0
No such names	0
Bad values	0

Note: If you click a performance group category and do not select a device, you will see the statistics for the last device loaded when you click View.

Viewing Data for Clusters

When viewing performance data for devices belonging 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. Below is an example of SNMP statistics shown for a cluster:



SNMP statistics for device sd115_sd114

sd114

Authentication traps	enabled
In packets	4909
Out packets	5640

SNMP inbound details

Bad versions	0
Bad community names	0
ASN parse errors	0
Silent drops	0
Too bigs	0
No such names	0
Bad values	0
Read only	0
General errors	0
Total requested variables	14361
Total set variables	0
Get requests	4
Get next requests	4521
Set requests	0
Get responses	0

sd115

Authentication traps	enabled
In packets	853
Out packets	1183

SNMP inbound details

Bad versions	0
Bad community names	0
ASN parse errors	0
Silent drops	0
Too bigs	0
No such names	0
Bad values	0
Read only	0
General errors	0
Total requested variables	3677
Total set variables	0
Get requests	2
Get next requests	729
Set requests	0
Get responses	0

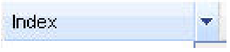
Customizing the Display

For the performance tables with columns of data, you can customize the data presented in the tables by changing the columns that are displayed and/or the order of the table entries.

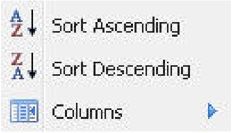
Customizing Column Data

To customize column data:

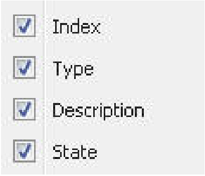
1. Position the cursor over a column heading. An arrow appears on the right hand side of the box. For example:



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



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



☑ Index
☑ Type
☑ Description
☑ State

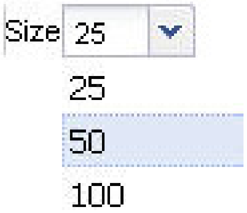
5. Click a marked checkbox to hide that column or click an empty checkbox to display that column.
6. Click elsewhere in the display to clear the menus.

Configuring the Number of Records

By default, 25 records are shown per page in the performance manager view.

To configure the number of records displayed:

1. At the top of the performance window, click the down arrow next to Size. The drop down list of values appears.

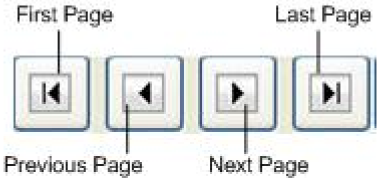


2. Click the number you want to apply.

Navigating Pages

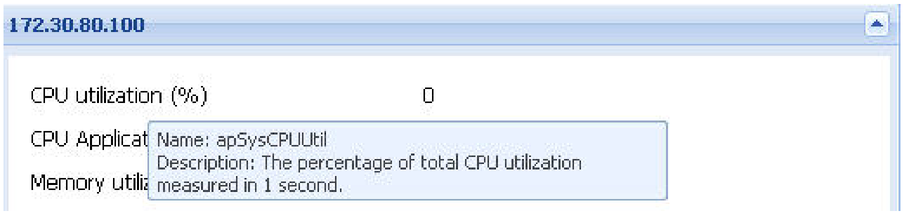
To navigate through multiple pages:

1. Use the navigation arrows located at the top of the performance manager window to navigate through multiple pages.
2. Click the navigation icons to display the desired page, such as the first page, previous page, next page, and the last page of list view.



Using Tool Tips

For definitions of the data categories in the performance windows, mouse over the data name and a tool tip will appear with an attribute name and definition. For example:



172.30.80.100

CPU utilization (%) 0

CPU Applicat

Memory utili

Name: apSysCPUUtil
Description: The percentage of total CPU utilization measured in 1 second.

Refreshing Data

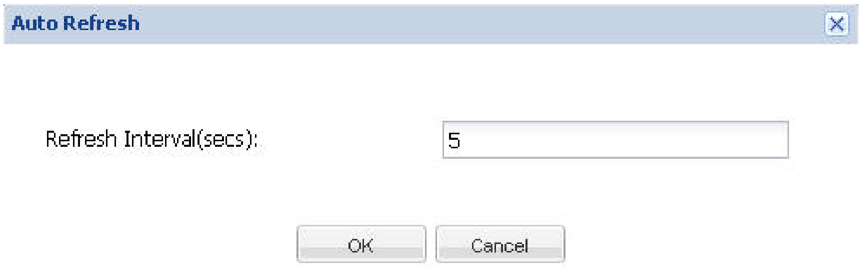
You can refresh the statistics displayed on each performance window by clicking Refresh.

Configuring Auto Refresh

You can configure auto refresh to refresh the data at a set interval.

To configure auto refresh:

1. Click Auto refresh. The Auto Refresh dialog box appears.
2. Refresh Interval(secs):—Enter the number of seconds you want to configure for auto refresh.



Refresh Interval(secs): 5

3. Click OK.
4. Click Cancel to cancel auto refresh configuration.

Stopping Auto Refresh

When Auto refresh is configured, Stop Auto Refresh becomes enabled.

To stop auto refresh:

Click Stop Auto Refresh. Auto refresh is disabled.

Saving Data

You can save the data displayed on each performance window to a text file in comma separated values (CSV) format.

To save data to a file:

1. With the data you want to save displayed, click Save to file. A Save window opens with a file name 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
   ```
2. Click OK to save the file and close the window.

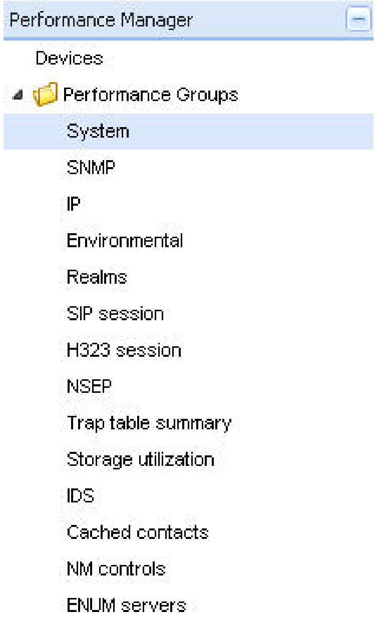
System

This section explains the system performance information displayed by Oracle Communications Session Delivery Manager.

Accessing System Data

To access System data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view system performance data.
3. Click View. The list of performance data appears.
4. Click System under the Performance Groups folder.



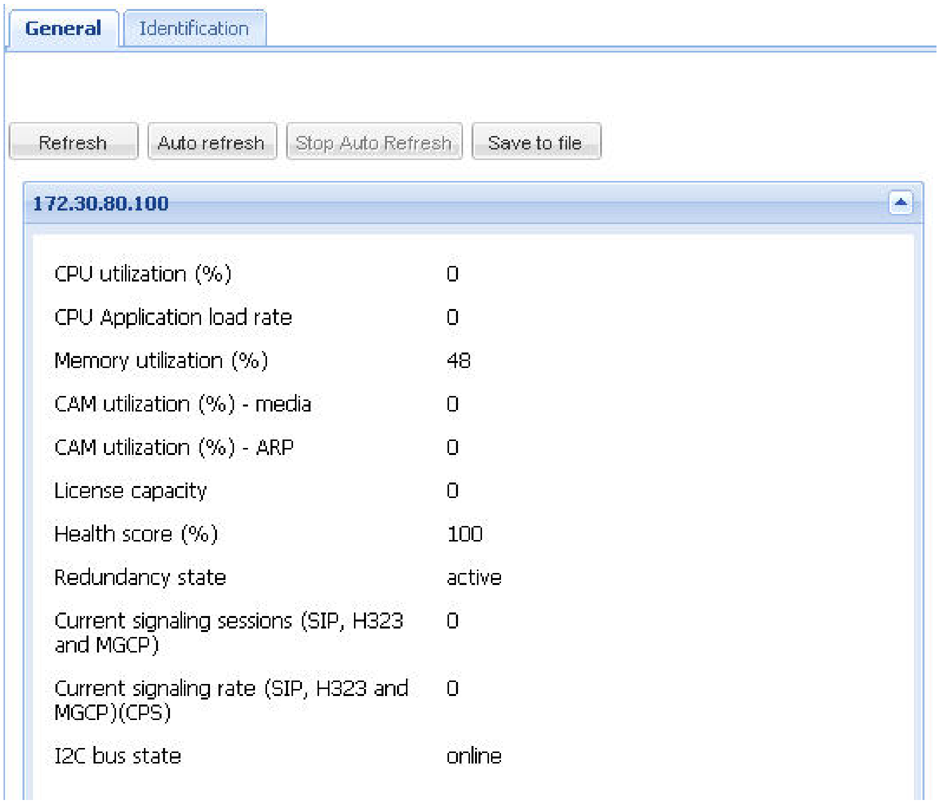
The system window appears in the content area with two tabs: General and Identification.

Note: For all performance categories with additional tabs of data, the window always opens to the first tab by default.

General Data

To access General data:

In the System window, click the General tab. The general system data appear:



CPU utilization (%)	0
CPU Application load rate	0
Memory utilization (%)	48
CAM utilization (%) - media	0
CAM utilization (%) - ARP	0
License capacity	0
Health score (%)	100
Redundancy state	active
Current signaling sessions (SIP, H323 and MGCP)	0
Current signaling rate (SIP, H323 and MGCP)(CPS)	0
I2C bus state	online

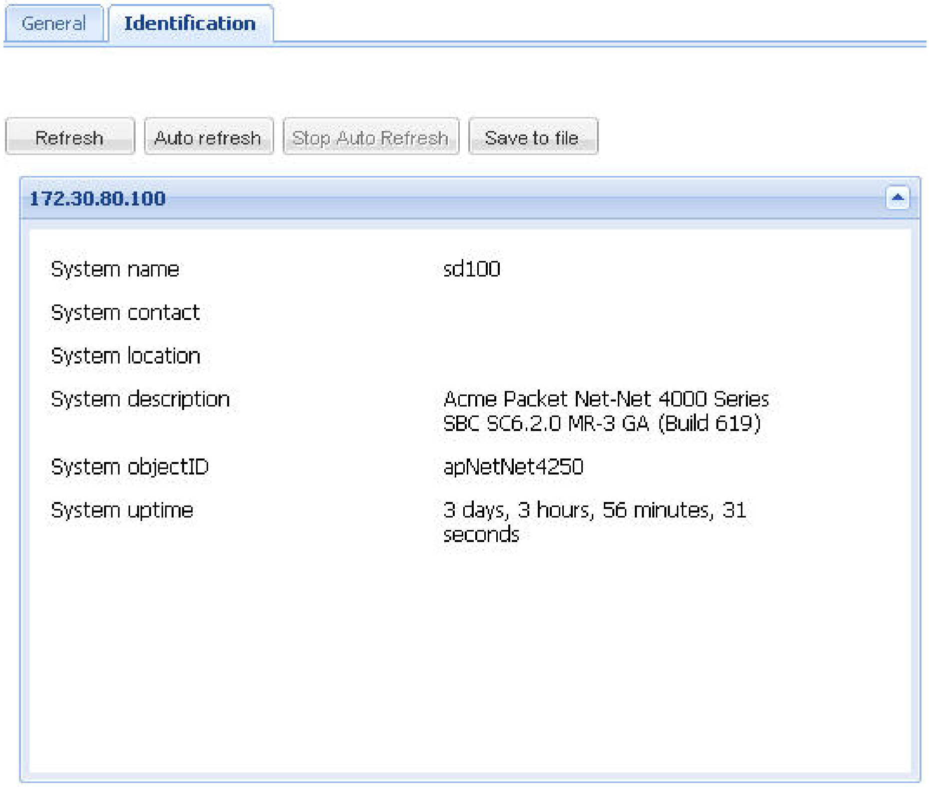
The following table defines the data displayed by Oracle Communications Session Delivery Manager:

Data	Description
CPU utilization (%)	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 (%)	Percentage of memory utilization
CAM utilization (%) - media	Percentage of NAT table in Content Addressable Memory (CAM) utilization
CAM utilization (%) - ARP	Percentage of ARP table (in CAM) utilization
License capacity	Percentage of licensed sessions currently in progress
Health score (%)	System health percentage, with a system health percentage value of 100 (100%) being the healthiest
Redundancy state	For clusters, information about the state of each device in the cluster. Values are: active standby
Current signaling sessions (SIP, H.323, and MGCP)	Total number of global concurrent sessions at the moment
Current signaling rate (SIP, H.323, and MGCP) (CPS)	Number of global calls per second
I2C bus state	State of the environmental monitor located in the chassis. Values are: online: Denotes regular call processing offline: Denotes no call processing but other administrative functions are available

Identification Data

To access Identification data:

In the System window, click the Identification tab. The system identification data appears:



System name	sd100
System contact	
System location	
System description	Acme Packet Net-Net 4000 Series SBC SC6.2.0 MR-3 GA (Build 619)
System objectID	apNetNet4250
System uptime	3 days, 3 hours, 56 minutes, 31 seconds

The following table defines the data:

Data	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

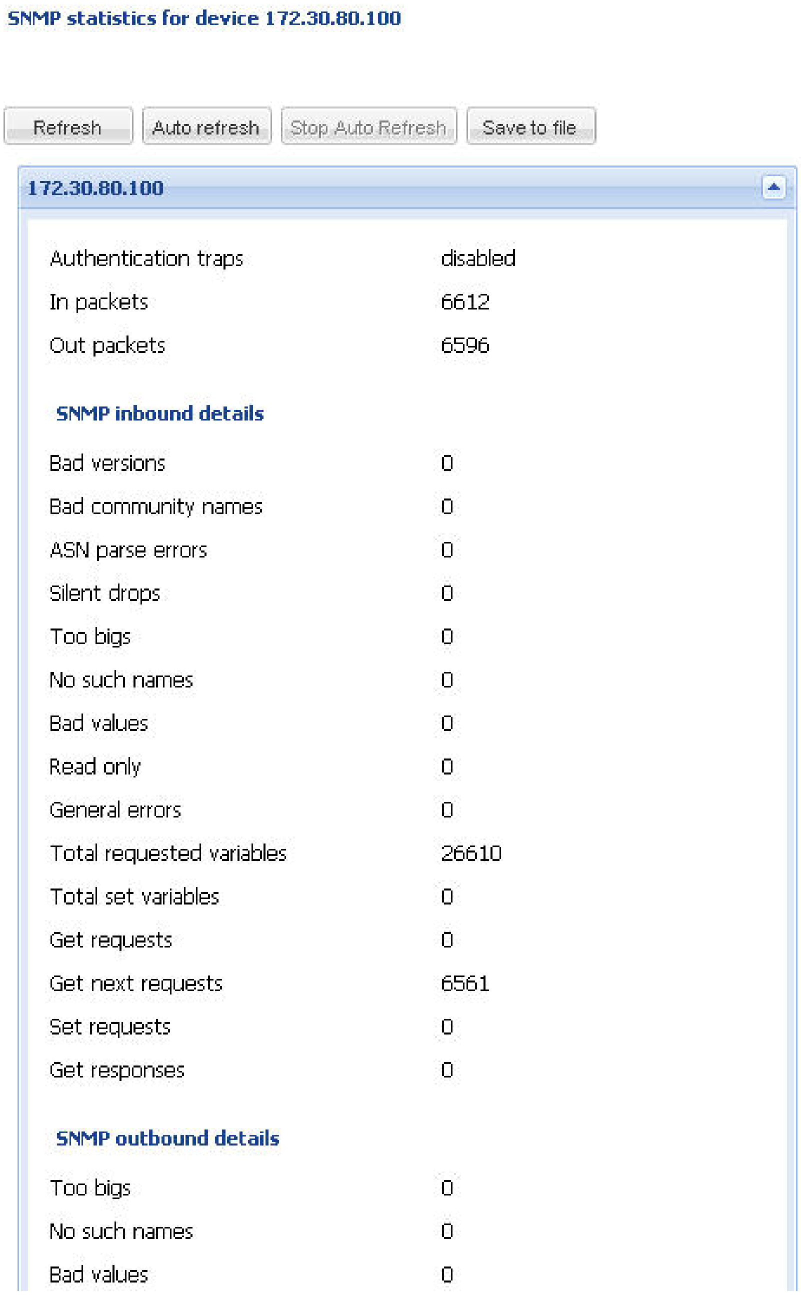
This section describes the SNMP performance data displayed by Oracle Communications Session Delivery Manager.

Accessing SNMP Data

To access SNMP data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view SNMP data.
3. Click View. The list of performance data appears.
4. Click SNMP under the Performance Groups folder.

   The SNMP window appears in the content area. The data is broken into three sections. Use the scroll bar to view data at the bottom of the content area.



SNMP statistics for device 172.30.80.100

172.30.80.100

Authentication traps	disabled
In packets	6612
Out packets	6596

SNMP inbound details

Bad versions	0
Bad community names	0
ASN parse errors	0
Silent drops	0
Too bigs	0
No such names	0
Bad values	0
Read only	0
General errors	0
Total requested variables	26610
Total set variables	0
Get requests	0
Get next requests	6561
Set requests	0
Get responses	0

SNMP outbound details

Too bigs	0
No such names	0
Bad values	0

The following table defines the information displayed:

Data	Description
Authentication traps	Indicates whether the SNMP entity is permitted to generate authenticationFailure traps

Data	Description
In packets	Total number of messages delivered to the SNMP entity from the transport service
Out packets	Total number of SNMP messages passed from the SNMP protocol entity to the transport service
Bad versions	Total number of SNMP messages delivered to the SNMP entity for an unsupported SNMP version
SNMP inbound details:	
Bad versions	Total number of SNMP messages which were delivered to the SNMP entity and were for an unsupported SNMP version
Bad community names	Total number of SNMP messages delivered to the SNMP entity which used a SNMP community name not known to said entity
Bad community uses	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	Total number of ASN.1 or BER errors encountered by the SNMP entity when decoding received SNMP messages
Silent drops	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	Total number of SNMP PDUs delivered to the SNMP protocol entity and for which the value of the error-status field is tooBig
No such names	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	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	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

Data	Description
General errors	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	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	Total number of MIB objects altered successfully by the SNMP protocol entity as the result of receiving valid SNMP set-Request PDUs
Get requests	Total number of SNMP Get-Request PDUs that have been accepted and processed by the SNMP protocol entity
Get next requests	Total number of SNMP Get-Next PDUs that have been accepted and processed by the SNMP protocol entity
Set requests	Total number of SNMP Set-Request PDUs that have been accepted and processed by the SNMP protocol entity
Get responses	Total number of SNMP Get-Responses that have been accepted and processed by the SNMP protocol entity
Traps	Total number of SNMP Trap PDUs that have been accepted and processed by the SNMP protocol entity
SNMP outbound details	
Too bigs	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	Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is noSuchName
Bad values	Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is badValue
General errors	Total number of SNMP PDUs generated by the SNMP protocol entity for which the value of the error-status field is genErr
Get responses	Total number of SNMP Get-Responses generated by the SNMP protocol entity
Traps	Total number of SNMP Trap PDUs generated by the SNMP protocol entity

IP

This section describes the IP data displayed by Oracle Communications Session Delivery Manager.

Accessing IP Data

To access IP data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view IP performance data.
3. Click View. The list of performance data appears.
4. Click IP under the Performance Groups folder.

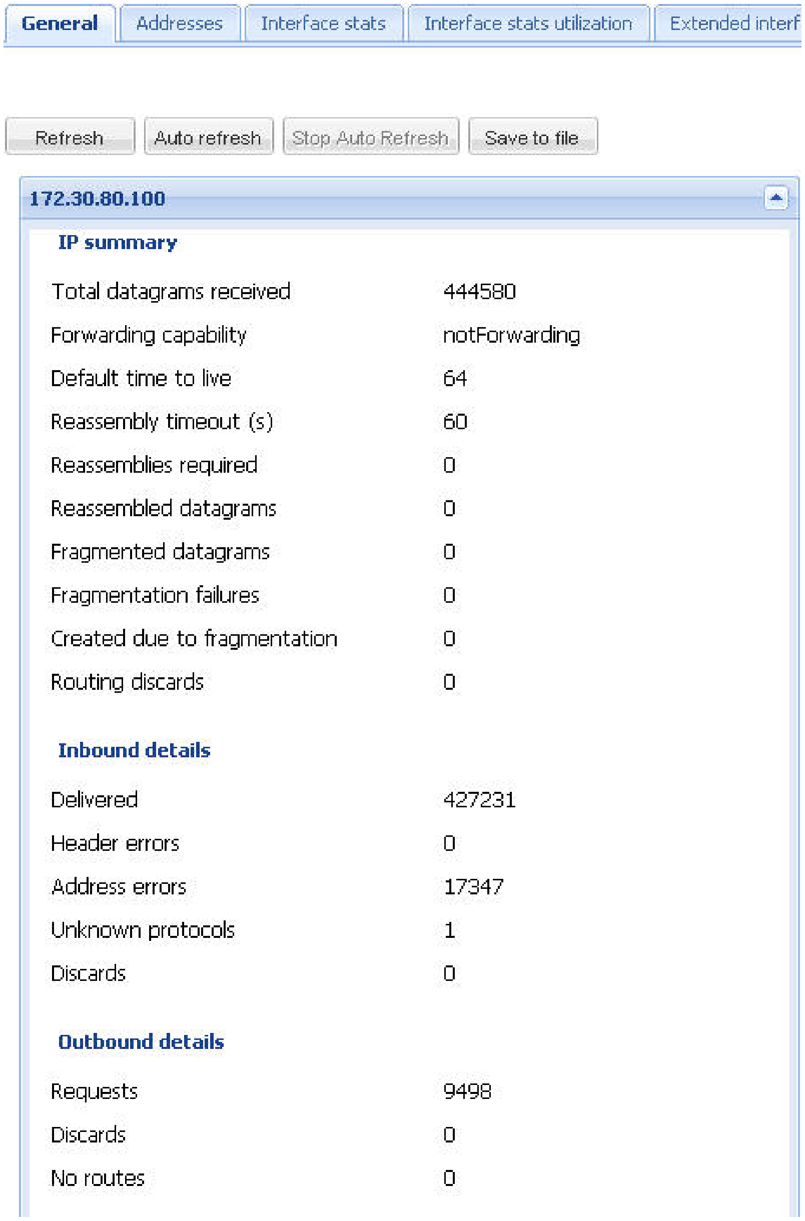
   The IP performance data appears for the following categories:

   - General: General performance data
   - Addresses: Information about this Net-Net SBC’s IP addressing
   - Interface stats: Information about the Net-Net SBC’s interfaces. Each interface is thought of as being attached to a subnetwork.
   - Interface stats utilization: Information related to RX utilization and TX utilzation of media ports
   - Extended interface stats: Information about the Net-Net SBC’s extended interfaces
   - ICMP: Information about this Net-Net SBC and Internet Control Message Protocol (ICMP)
   - Global TCP: Information about this Net-Net SBC’s existing global TCP connections
   - TCP: Information about this Net-Net SBC’s existing TCP connections
   - UDP: Information about this Net-Net SBC’s UDP end-points, upon which a local application is currently accepting datagrams

General

To access General data:

In the IP window, click the General tab. The following data appears:



172.30.80.100

IP summary

Total datagrams received	444580
Forwarding capability	notForwarding
Default time to live	64
Reassembly timeout (s)	60
Reassemblies required	0
Reassembled datagrams	0
Fragmented datagrams	0
Fragmentation failures	0
Created due to fragmentation	0
Routing discards	0

Inbound details

Delivered	427231
Header errors	0
Address errors	17347
Unknown protocols	1
Discards	0

Outbound details

Requests	9498
Discards	0
No routes	0

The following table defines the data displayed:

Data	Description
IP summary	
Total datagrams received	Total number of input datagrams received from interfaces, including those received in error
Forwarding capability	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

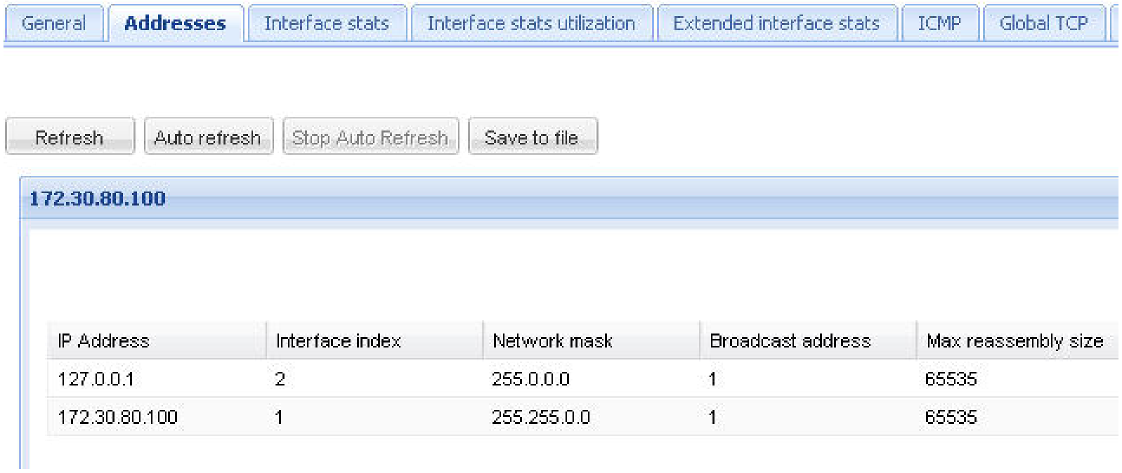
Data	Description
Default time-to-live	Default value inserted into the Time-To-Live (TTL) field of the IP header of datagrams originated at this entity, whenever a TTL value is not supplied by the transport layer protocol
Reassembly timeout(s)	Maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity
Reassemblies required	Number of IP fragments received which needed to be reassembled at this entity
Reassembled datagrams	Number of IP datagrams successfully re-assembled
Fragmented datagrams	Number of IP datagrams that have been successfully fragmented at this entity
Fragmentation failures	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	Number of IP datagram fragments that have been generated as a result of fragmentation at this entity
Routing discards	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	
Delivered	Total number of input datagrams successfully delivered to IP user-protocols including Internet Control Message Protocol (ICMP)
Header errors	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
Address errors	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	Number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol
Discards	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 that this counter does not include any datagrams discarded while awaiting re-assembly.)
Outbound details	
Requests	Total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission. (Note that this counter does not include any datagrams counted in ipForwDatagrams.)
Discards	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 that this counter would include

Data	Description
	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 that 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.)

Addresses

To access Addresses data:

In the IP window, click the Addresses tab. The following data appears:



IP Address	Interface index	Network mask	Broadcast address	Max reassembly size
127.0.0.1	2	255.0.0.0	1	65535
172.30.80.100	1	255.255.0.0	1	65535

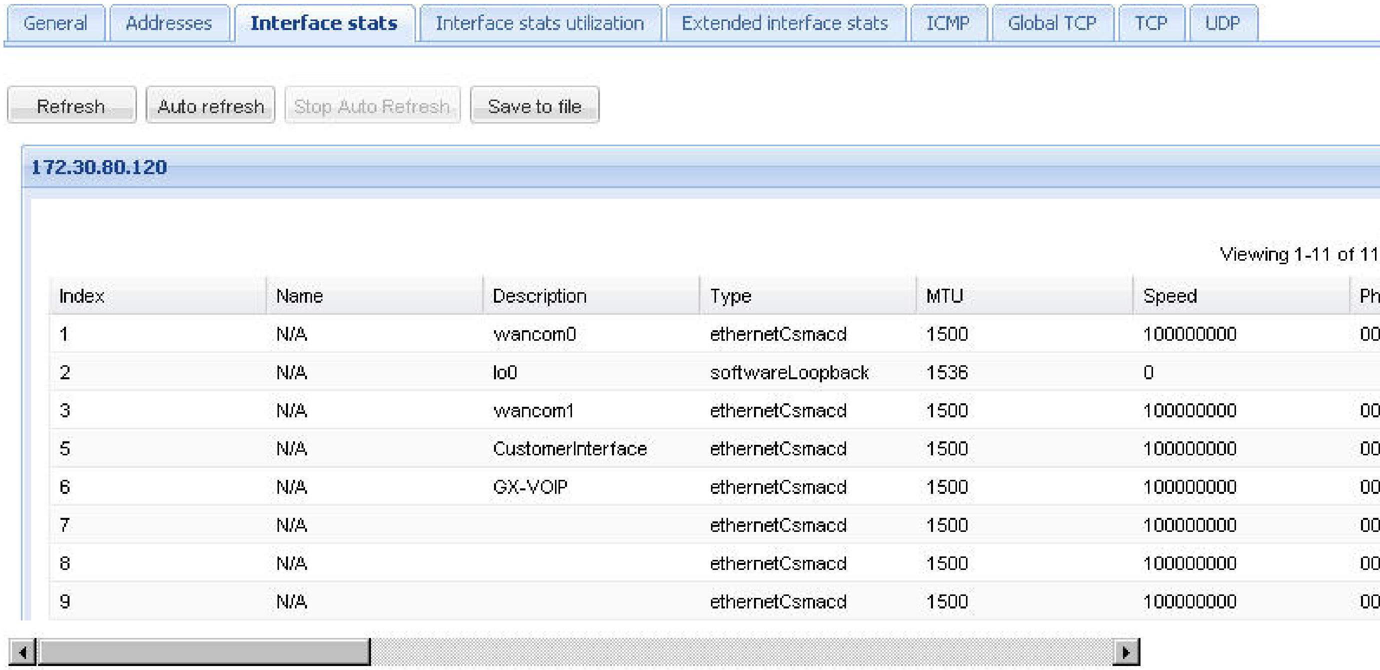
The following table defines the information displayed for the Net-Net system’s control and maintenance interfaces (such as wancom and loopback):

Data	Description
IP Address	IP address to which this entry's addressing information pertains
Interface Index	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	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	Size of the largest IP datagram which this entity can re-assemble from incoming IP fragmented datagrams received on this interface

Interface Stats

To access Interface stats data:

In the IP window, click the Interfaces stats tab. The following data appears:



172.30.80.120

Viewing 1-11 of 11

Index	Name	Description	Type	MTU	Speed	Ph
1	N/A	wancom0	ethernetCsmacd	1500	100000000	00
2	N/A	lo0	softwareLoopback	1536	0	
3	N/A	wancom1	ethernetCsmacd	1500	100000000	00
5	N/A	CustomerInterface	ethernetCsmacd	1500	100000000	00
6	N/A	GX-VOIP	ethernetCsmacd	1500	100000000	00
7	N/A		ethernetCsmacd	1500	100000000	00
8	N/A		ethernetCsmacd	1500	100000000	00
9	N/A		ethernetCsmacd	1500	100000000	00

Use the scroll bar to view all data.

The following table defines the information displayed in the Interface stats tab.

Data	Description
Index	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	Name of this STD interface
Description	Textual 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	Information about the type of interface, distinguished according to the physical/link protocol(s) immediately below the network layer in the protocol stack
MTU	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	Estimate of the interface's current bandwidth 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	Interface's address 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. Values are: up down testing

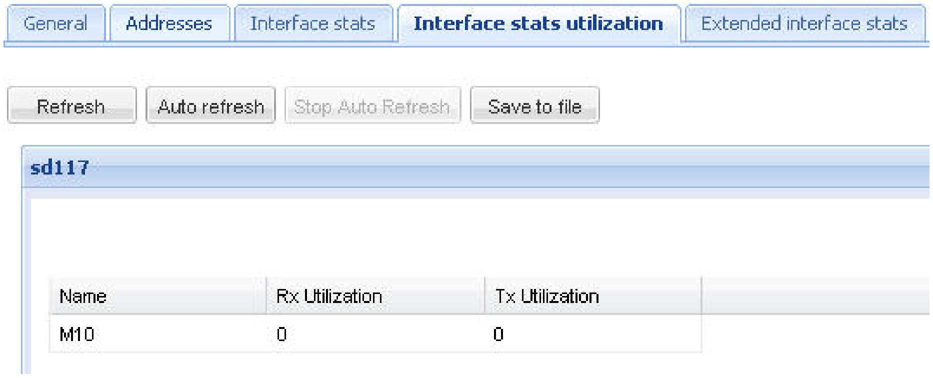
Data	Description
Operational status	Current operational state of the interface. Values are: up down testing
Last change time	Value of sysUpTime at the time the interface entered its current operational state. If the current state was entered prior to the last re-initialization of the local network management subsystem, then it contains a zero value
In	
Octets	Total number of octets received on the interface, including framing characters
Unicast pkts	Number of subnetwork-unicast packets delivered to a higher-layer protocol
Non-Unicast pkts	Number of non-unicast (for example, subnetwork-broadcast or subnetwork-multicast) packets delivered to a higher-layer protocol
Discards	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
Errors	Number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol
Unknown protocols	For packet-oriented interfaces, the number of packets received via 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 will always be zero
Out	
Octets	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 pkts	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 pkts	Total number of packets that higher-level protocols requested be transmitted to a non-unicast (i.e., a subnetwork-broadcast or subnetwork-multicast) address, including those that were discarded or not sent
Discards	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
Errors	Number of outbound packets that could not be transmitted because of errors

Interface Stats Utilization

To access Interface stats utilization data:

In the IP window, click the Interfaces stats utilization tab.

The following data related to RX utilization and TX utilzation of media ports appears:



Name	Rx Utilization	Tx Utilization
M10	0	0

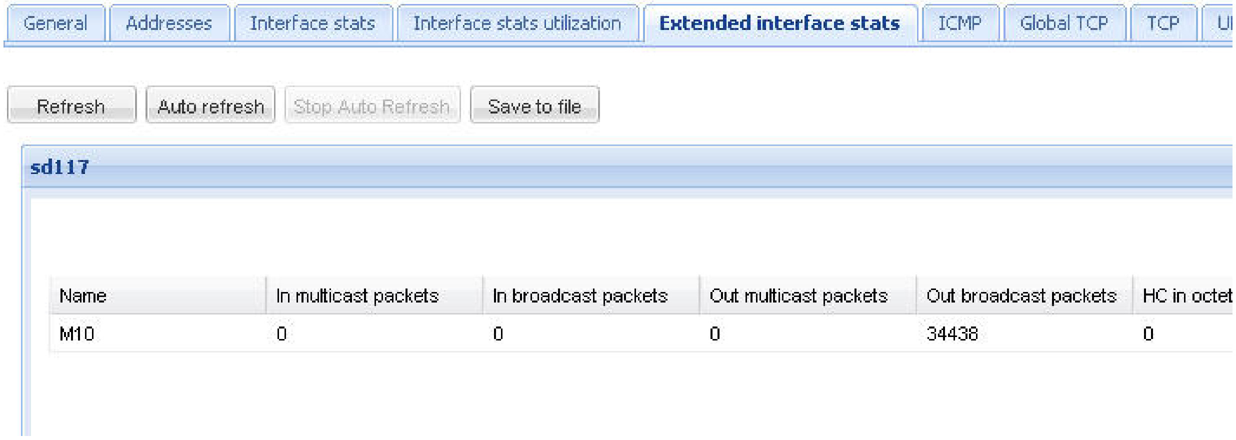
The following table defines the information displayed in the Utilization tab.

Data	Description
Name	Textual 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
Rx Utilization	RX utilization of media ports indexed by IF index
Tx Utilization	TX utilization of media ports indexed by IF index

Extended Interface Stats

To access extended interface stats data:

In the IP window, click the Extended interfaces stats tab. The following data appears:



Name	In multicast packets	In broadcast packets	Out multicast packets	Out broadcast packets	HC in octet
M10	0	0	0	34438	0

Use the scroll bar at the bottom of the content area to view all data.

The following table defines the information displayed for the Net-Net 9000’s media interfaces:

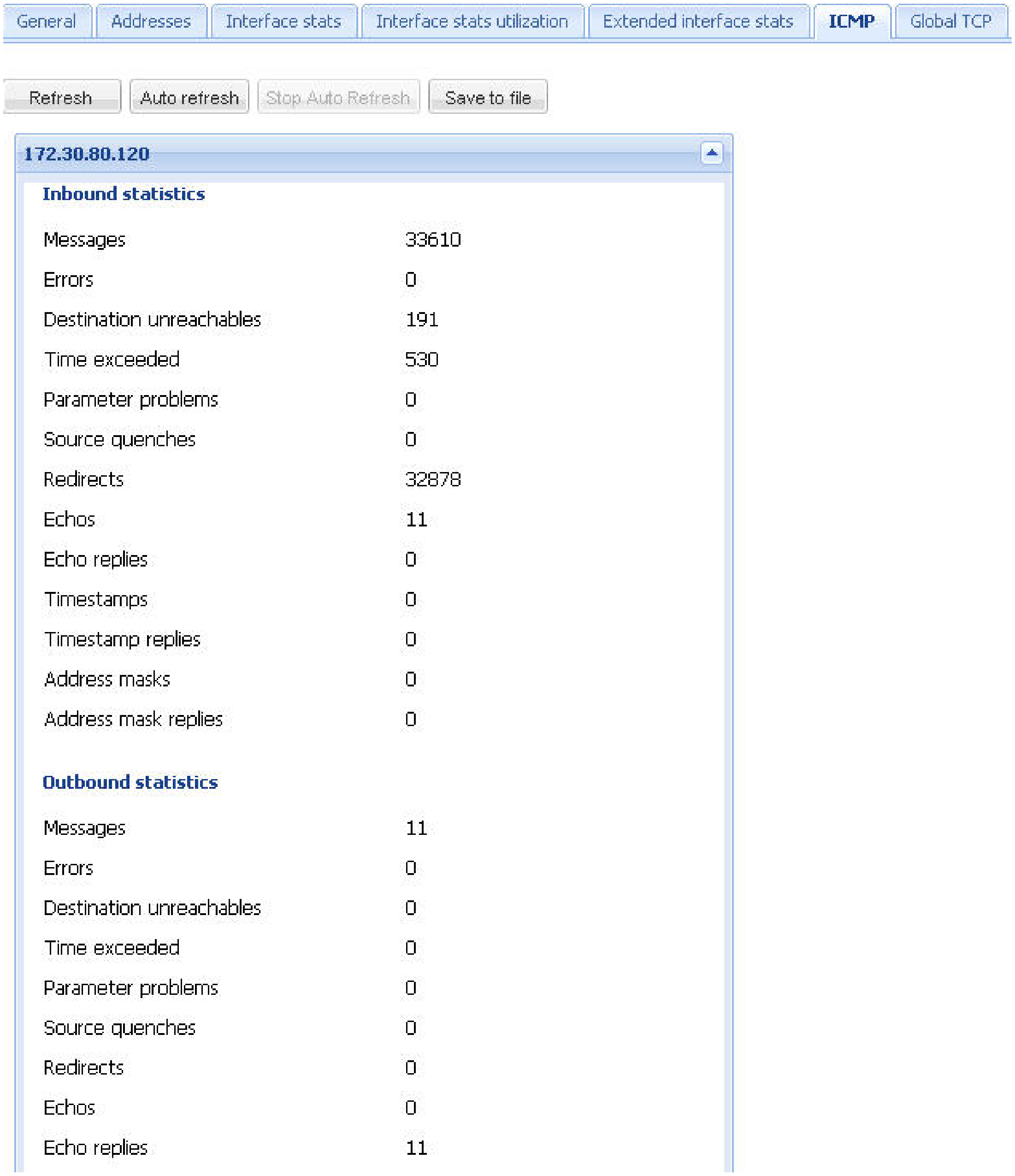
Data	Description
Name	Textual string containing the name of the interface. The name is the one assigned by the local device. It could be a text name or a port number, depending on the interface naming syntax of the device
In	
Multicast packets	Number of packets delivered from this layer to a higher layer that were addressed to a multicast address. For a MAC layer protocol, it includes both group and functional addresses
Broadcast packets	Number of packets delivered by this layer to a higher level that were addressed to a broadcast address
Out	
Multicast packets	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	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	
Octets	Total number of octets received on the interface, including framing characters
Unicast packets	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	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	Number of packets delivered by this layer to a higher layer that were addressed to a broadcast address at this layer
HC out	
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	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	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	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

Data	Description
High Speed	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)

ICMP

To access ICMP data:

In the IP window, click the ICMP tab. The following data appears:



172.30.80.120

Inbound statistics

Messages	33610
Errors	0
Destination unreachables	191
Time exceeded	530
Parameter problems	0
Source quenches	0
Redirects	32878
Echos	11
Echo replies	0
Timestamps	0
Timestamp replies	0
Address masks	0
Address mask replies	0

Outbound statistics

Messages	11
Errors	0
Destination unreachables	0
Time exceeded	0
Parameter problems	0
Source quenches	0
Redirects	0
Echos	0
Echo replies	11

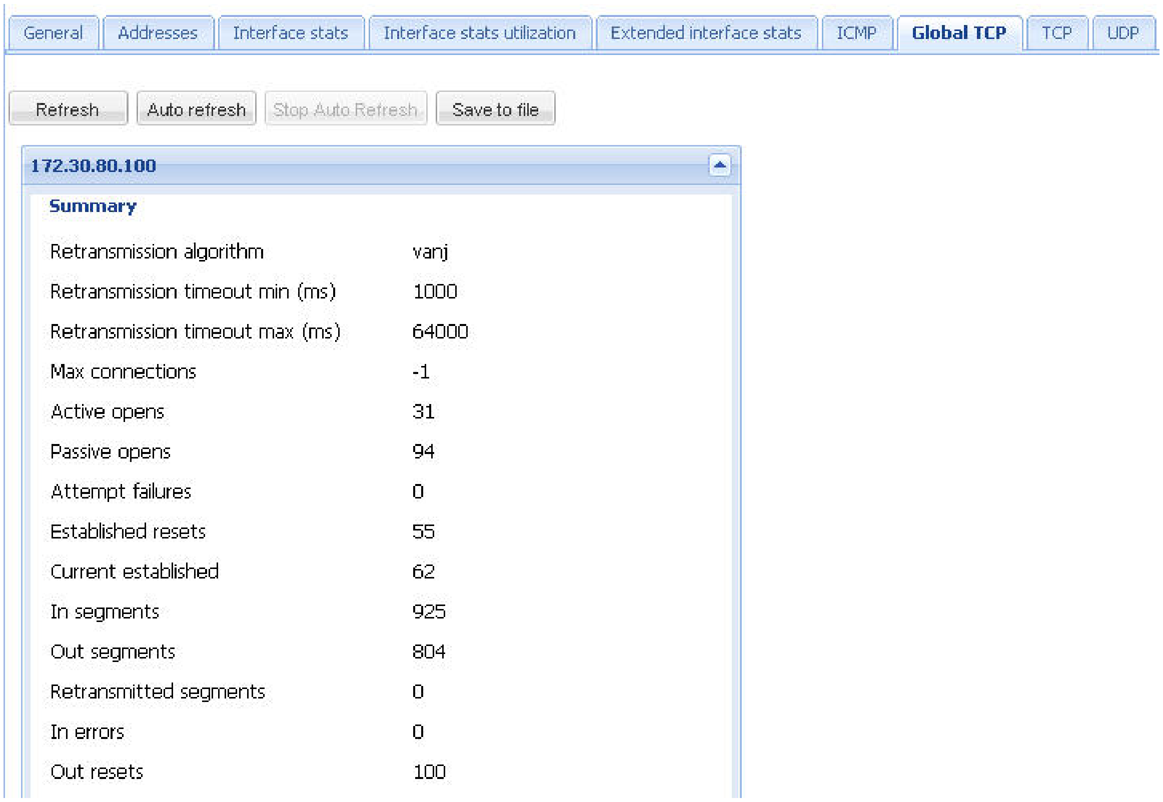
The following table defines the information displayed:

Data	Description
Inbound statistics	
Messages	Total number of ICMP messages which the Net-Net SBC received. (Note that this counter includes all those counted by icmpInErrors.)
Errors	Number of ICMP messages which the Net-Net SBC received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on)
Destination unreachables	Number of ICMP Destination Unreachable messages received
Time exceeded	Number of ICMP Time Exceeded messages received
Parameter problems	Number of ICMP Parameter Problem messages received
Source quenches	Number of ICMP Source Quench messages received
Redirects	Number of ICMP Redirect messages received
Echoes	Number of ICMP Echo (request) messages received
Echo replies	Number of ICMP Echo Reply messages received
Timestamps	Number of ICMP Timestamp (request) messages received
Timestamp replies	Number of ICMP Timestamp Reply messages received
Address masks	Number of ICMP Address Mask Request messages received
Address mask replies	Number of ICMP Address Mask Reply messages received
Outbound statistics	
Messages	Total number of ICMP messages which the Net-Net SBC attempted to send. (This counter includes all those counted by icmpOutErrors.)
Errors	Number of ICMP messages which the Net-Net SBC 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	Number of ICMP Destination Unreachable messages sent
Time exceeded	Number of ICMP Time Exceeded messages sent
Parameter problems	Number of ICMP Parameter Problem messages sent
Source quenches	Number of ICMP Source Quench messages sent
Redirects	Number of ICMP Redirect messages sent
Echoes	Number of ICMP Echo (request) messages sent
Echo replies	Number of ICMP Echo Reply messages sent
Timestamps	Number of ICMP Timestamp (request) messages sent
Timestamp replies	Number of ICMP Timestamp Reply messages sent
Address masks	Number of ICMP Address Mask Request messages sent
Address mask replies	Number of ICMP Address Mask Reply messages sent

Global TCP

To access global TCP data:

In the IP window, click the Global TCP tab. The following data appears:



Retransmission algorithm	vanj
Retransmission timeout min (ms)	1000
Retransmission timeout max (ms)	64000
Max connections	-1
Active opens	31
Passive opens	94
Attempt failures	0
Established resets	55
Current established	62
In segments	925
Out segments	804
Retransmitted segments	0
In errors	0
Out resets	100

The following table defines the information displayed:

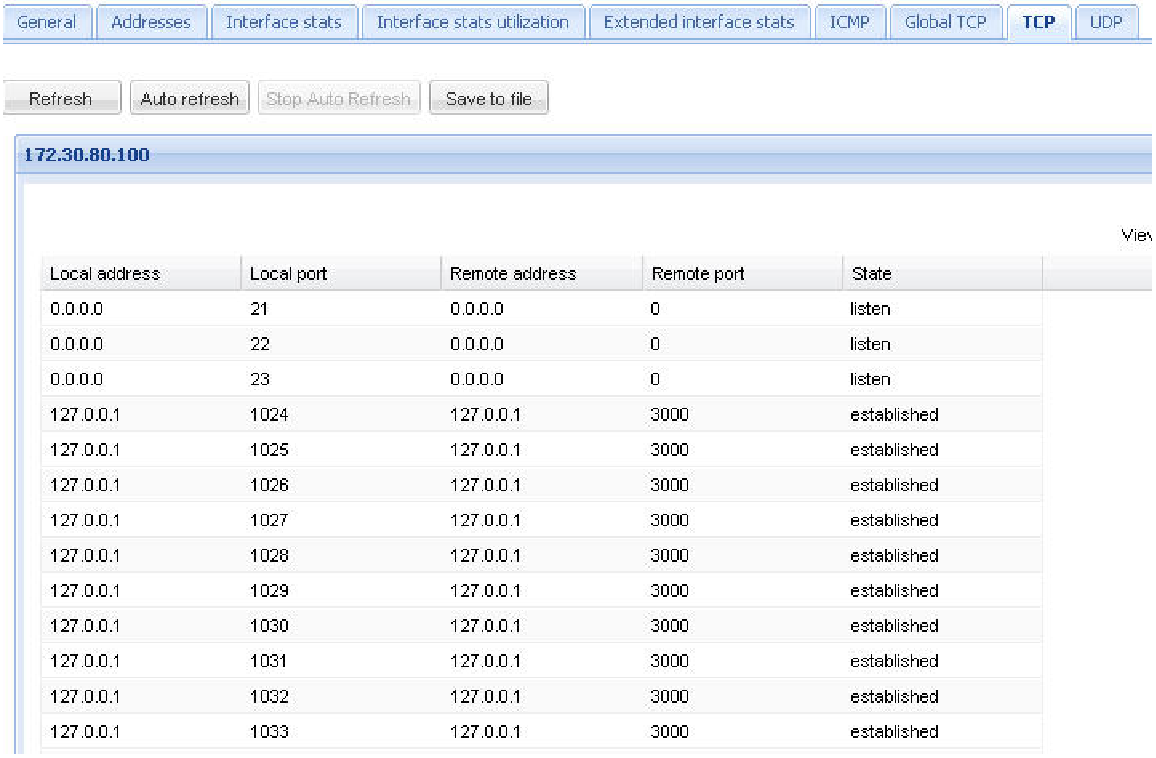
Data	Description
Retransmission algorithm	Algorithm used to determine the timeout value used for retransmitting unacknowledged octets
Retransmission timeout min (ms)	Minimum value permitted by a TCP implementation for the retransmission timeout, measured in milliseconds. More refined semantics for objects 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)	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	Total number of TCP connections the Net-Net SBC supports. In entities where the maximum number of connections is dynamic, this object contains the value -1
Active opens	Number of times TCP connections made a direct transition to the SYN-SENT state from the CLOSED state
Passive opens	Number of times TCP connections made a direct transition to the SYN-RCVD state from the LISTEN state

Data	Description
Attempt fails	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	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	Number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT
In segments	Total number of segments received, including those received in error. This count includes segments received on currently established connections
Out segments	Total number of segments sent, including those on current connections but excluding those containing only retransmitted octets
Retransmitted segments	Total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets
In errors	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	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

TCP

To access TCP data:

In the IP window, click the TCP tab. The following data appears:



Local address	Local port	Remote address	Remote port	State
0.0.0.0	21	0.0.0.0	0	listen
0.0.0.0	22	0.0.0.0	0	listen
0.0.0.0	23	0.0.0.0	0	listen
127.0.0.1	1024	127.0.0.1	3000	established
127.0.0.1	1025	127.0.0.1	3000	established
127.0.0.1	1026	127.0.0.1	3000	established
127.0.0.1	1027	127.0.0.1	3000	established
127.0.0.1	1028	127.0.0.1	3000	established
127.0.0.1	1029	127.0.0.1	3000	established
127.0.0.1	1030	127.0.0.1	3000	established
127.0.0.1	1031	127.0.0.1	3000	established
127.0.0.1	1032	127.0.0.1	3000	established
127.0.0.1	1033	127.0.0.1	3000	established

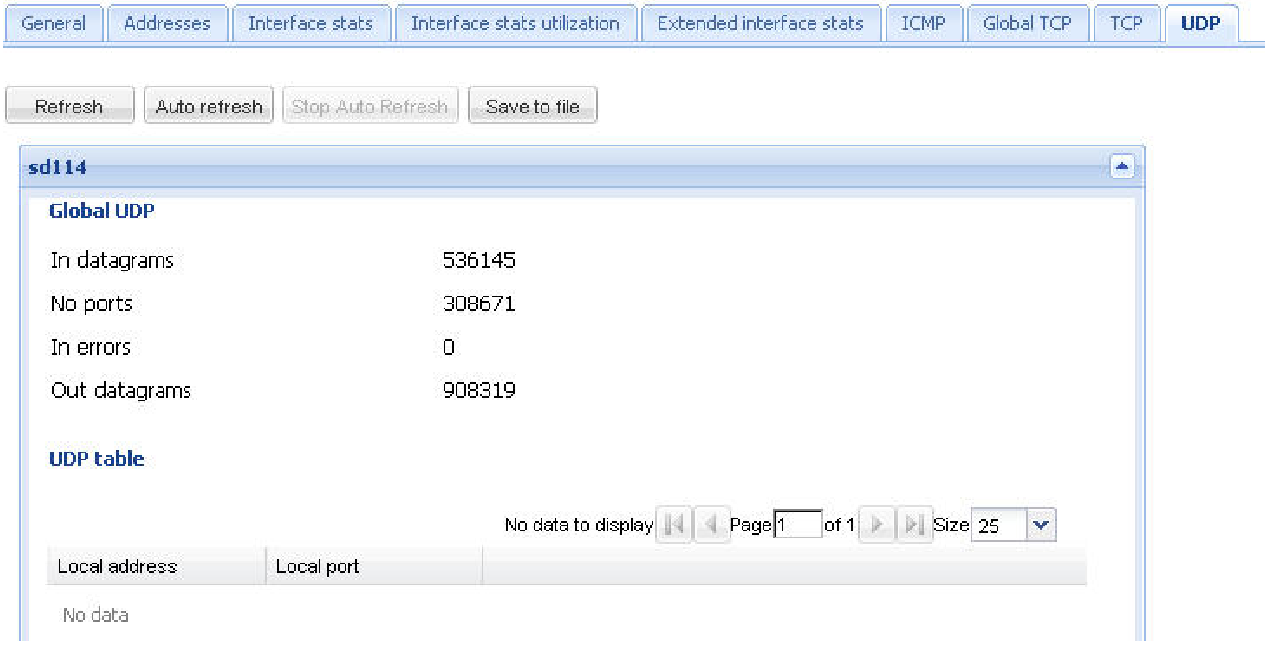
The following table defines the information displayed:

Data	Description
Local address	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	Local port number for this TCP connection
Remote address	Remote IP address for this TCP connection
Remote port	Remote port number for this TCP connection
State	State of this TCP connection. Values are: closed listen established

UDP

To access UDP data:

In the IP window, click the UDP tab. The following data appears:



Global UDP

In datagrams	536145
No ports	308671
In errors	0
Out datagrams	908319

UDP table

No data to display Page 1 of 1 Size 25

Local address	Local port
No data	

No data indicates there is no performance data for this performance category for this device.

The following table defines the information displayed:

Data	Description
Global UDP	
In datagrams	Total number of UDP datagrams delivered to UDP users
No ports	Total number of received UDP datagrams for which there was no application at the destination port
In errors	Number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port

Data	Description
Out datagrams	Total number of UDP datagrams sent from this Net-Net SBC
UDP table	
Local address	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	Local port number for this UDP listener

Environmental

This section describes the environmental information displayed by Oracle Communications Session Delivery Manager.

Accessing Environmental Data

To access environmental data:

1. Expand the Performance Manager slider.
2. Click Devices and click the device in the device table for which you want to view environmental data.
3. Click View. The list of performance data appears.
4. Click Environmental under the Performance Groups folder.

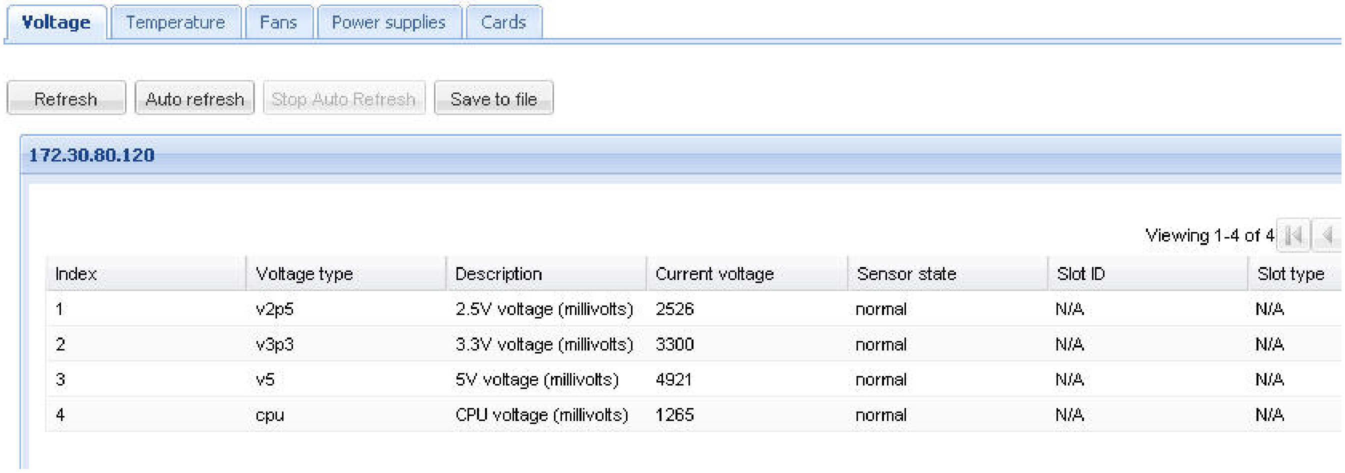
   The environmental performance data appears for the following categories:

   - Voltage
   - Temperature
   - Fans
   - Power supplies
   - Cards

Voltage

To access Voltage data:

In the Environmental window, click the Voltage tab. The following data appears:



Index	Voltage type	Description	Current voltage	Sensor state	Slot ID	Slot type
1	v2p5	2.5V voltage (millivolts)	2526	normal	N/A	N/A
2	v3p3	3.3V voltage (millivolts)	3300	normal	N/A	N/A
3	v5	5V voltage (millivolts)	4921	normal	N/A	N/A
4	cpu	CPU voltage (millivolts)	1265	normal	N/A	N/A

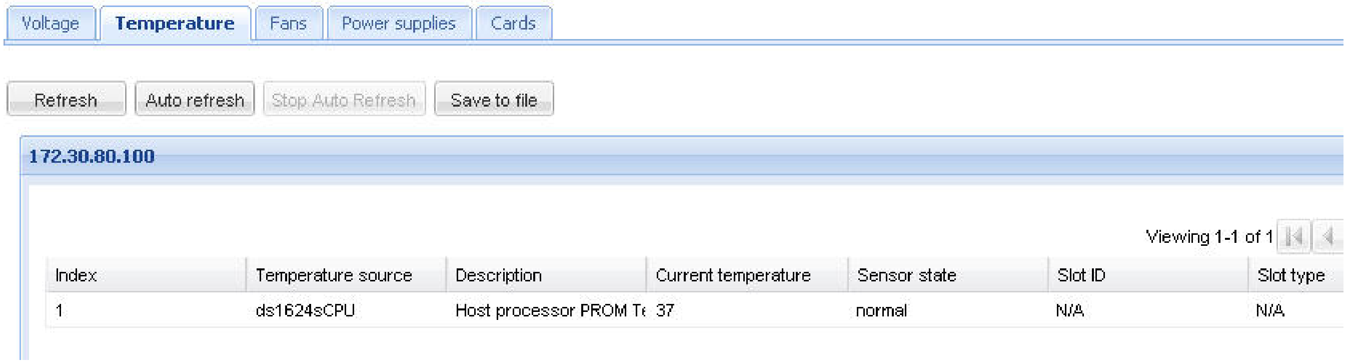
The following table defines the information displayed:

Data	Description
Index	A monotonically 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	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)	Current voltage measurement, in millivolts, if available. A value of -1 indicates that the monitor cannot obtain a value
Sensor state	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 minor range: 1.00v to 1.25v or 1.35v to 1.6v shutdown range: <1.0v or >1.6v
Slot ID	The slot this voltage is found on
Slot type	The type of module found in this slot

Temperature

To access Temperature data:

In the Environmental window, click the Temperature tab. The following data appears:



Index	Temperature source	Description	Current temperature	Sensor state	Slot ID	Slot type
1	ds1624sCPU	Host processor PROM Te	37	normal	N/A	N/A

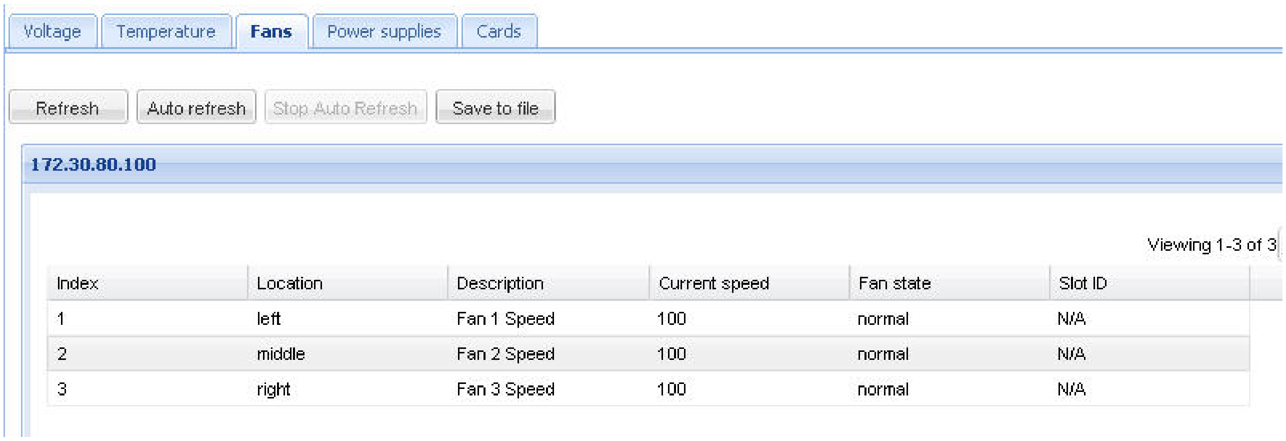
The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1
Temperature source	Indicates the entity being monitored for temperature
Description	Description of the temperature being monitored
Current temperature (degrees Celsius)	The current temperature of the main board PROM in Celsius
Sensor state	Current state of the temperature which can have one of the following values: initial: temperature is at its initial state normal: temperature is normal minor alarm: temperature is greater than or equal to 53 degrees Celsius and less than 63 degrees Celsius major alarm: temperature is greater than or equal to 63 degrees Celsius and less than 73 degrees Celsius critical alarm: temperature is greater than 73 degrees Celsius shutdown: system should be shutdown immediately not present: temperature sensor does not exist not functioning: temperature sensor is not functioning properly unknown: cannot obtain information due to an internal error
Slot ID	The slot this temperature is found on
Slot type	The type of module found in this slot

Fans

To access fan data:

In the Environmental window, click the Fans tab. The following data appears:



Index	Location	Description	Current speed	Fan state	Slot ID
1	left	Fan 1 Speed	100	normal	N/A
2	middle	Fan 2 Speed	100	normal	N/A
3	right	Fan 3 Speed	100	normal	N/A

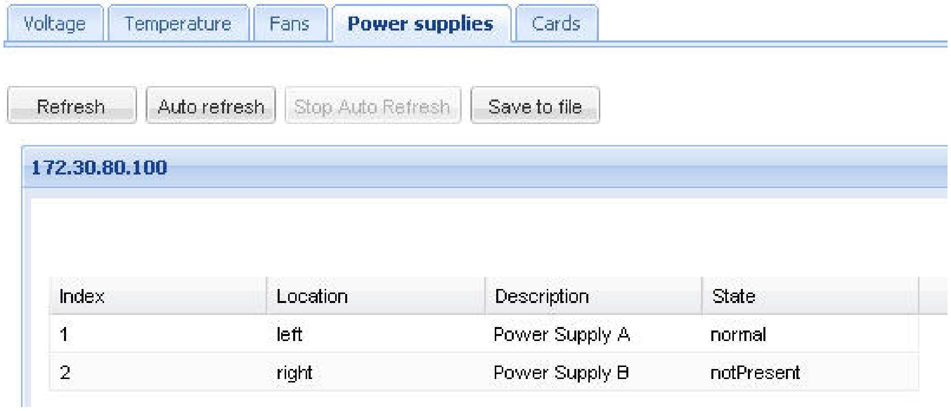
The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1
Location	Location of the fan. Values are: left fan middle fan right fan
Description	Description of the fan. Values are: fan 1 fan 2 fan 3
Current speed (% or range)	Current measurement of fan speed in percentage
Fan state	Current state of the fan speed. 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: fan sensor is not functioning properly unknown: cannot obtain information due to an internal error
Slot ID	The slot this fan is found in

Power Supplies

To access Power supplies data:

In the Environmental window, click the Power supplies tab. The following data appears:



Index	Location	Description	State
1	left	Power Supply A	normal
2	right	Power Supply B	notPresent

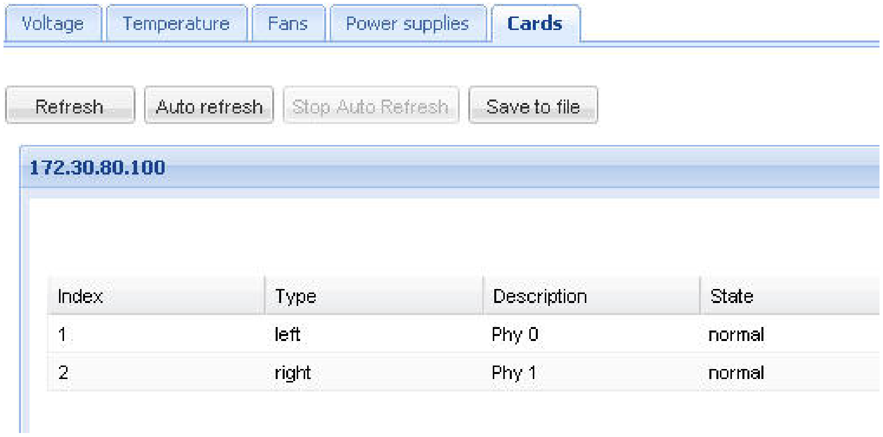
The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1
Location	Location of the power supply. Values are: Left power supply (A) Right power supply (B)
Description	Description of the power supply. Values are: Power supply A Power supply B
State	Current state of the power supply. Values are: normal: the power supply is normal unknown: the power supply sensor does not exist

Cards

To access card data:

In the Environmental window, click the Cards tab. The following data appears:



Index	Type	Description	State
1	left	Phy 0	normal
2	right	Phy 1	normal

The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer. When it reaches the maximum value the agent wraps the value back to 1
Type	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: state of the phy card is normal unknown: phy card is not present

Realms

This section describes the realms data displayed by Oracle Communications Session Delivery Manager.

Accessing Realms Data

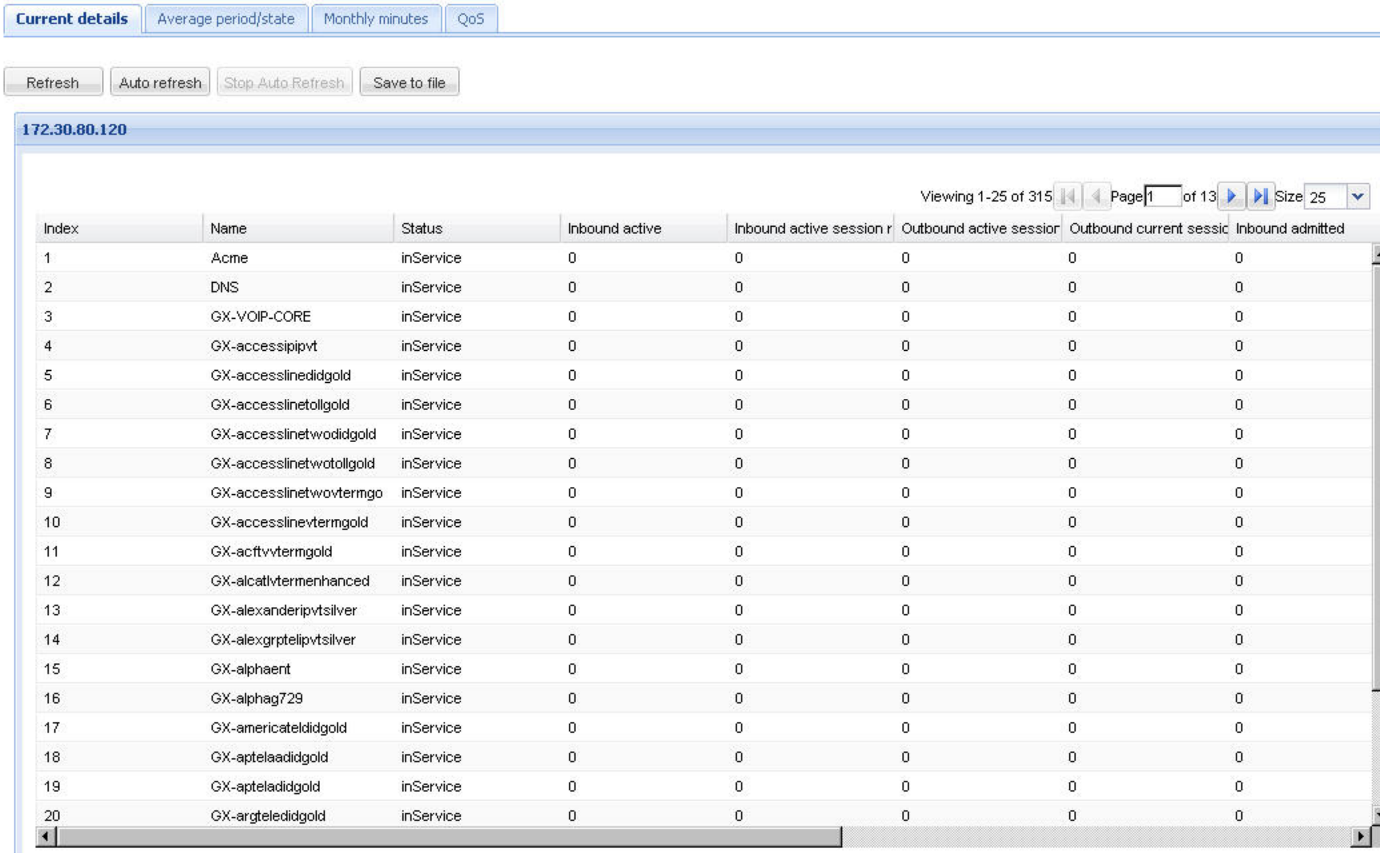
To access realms data:

1. Expand the Performance Manager slider.
2. Click Devices and click the device in the device table for which you want to view realms data.
3. Click View. The list of performance data appears.
4. Click Realms under the Performance Groups folder. The realms data appears for the following categories:
   - Current details
   - Average period/state
   - Monthly minutes
   - QoS

Current Details

To access current details data:

In the Realms window, click the Current details tab. The following data appears:



Index	Name	Status	Inbound active	Inbound active session r	Outbound active sessior	Outbound current sessic	Inbound admitted
1	Acme	inService	0	0	0	0	0
2	DNS	inService	0	0	0	0	0
3	GX-VOIP-CORE	inService	0	0	0	0	0
4	GX-accessipipvt	inService	0	0	0	0	0
5	GX-accesslinedidgold	inService	0	0	0	0	0
6	GX-accesslinetollgold	inService	0	0	0	0	0
7	GX-accesslinetwodidgold	inService	0	0	0	0	0
8	GX-accesslinetwotollgold	inService	0	0	0	0	0
9	GX-accesslinetwovtermgo	inService	0	0	0	0	0
10	GX-accesslinevtermgold	inService	0	0	0	0	0
11	GX-acftvvtermgold	inService	0	0	0	0	0
12	GX-alcatlvtermenhanced	inService	0	0	0	0	0
13	GX-alexanderipvtsilver	inService	0	0	0	0	0
14	GX-alexgrptelipvtsilver	inService	0	0	0	0	0
15	GX-alphaent	inService	0	0	0	0	0
16	GX-alphag729	inService	0	0	0	0	0
17	GX-americateldidgold	inService	0	0	0	0	0
18	GX-aptelaadidgold	inService	0	0	0	0	0
19	GX-apteladidgold	inService	0	0	0	0	0
20	GX-argteledidgold	inService	0	0	0	0	0

Use the horizontal and vertical scroll bars to view all data.

The following table defines the information displayed:

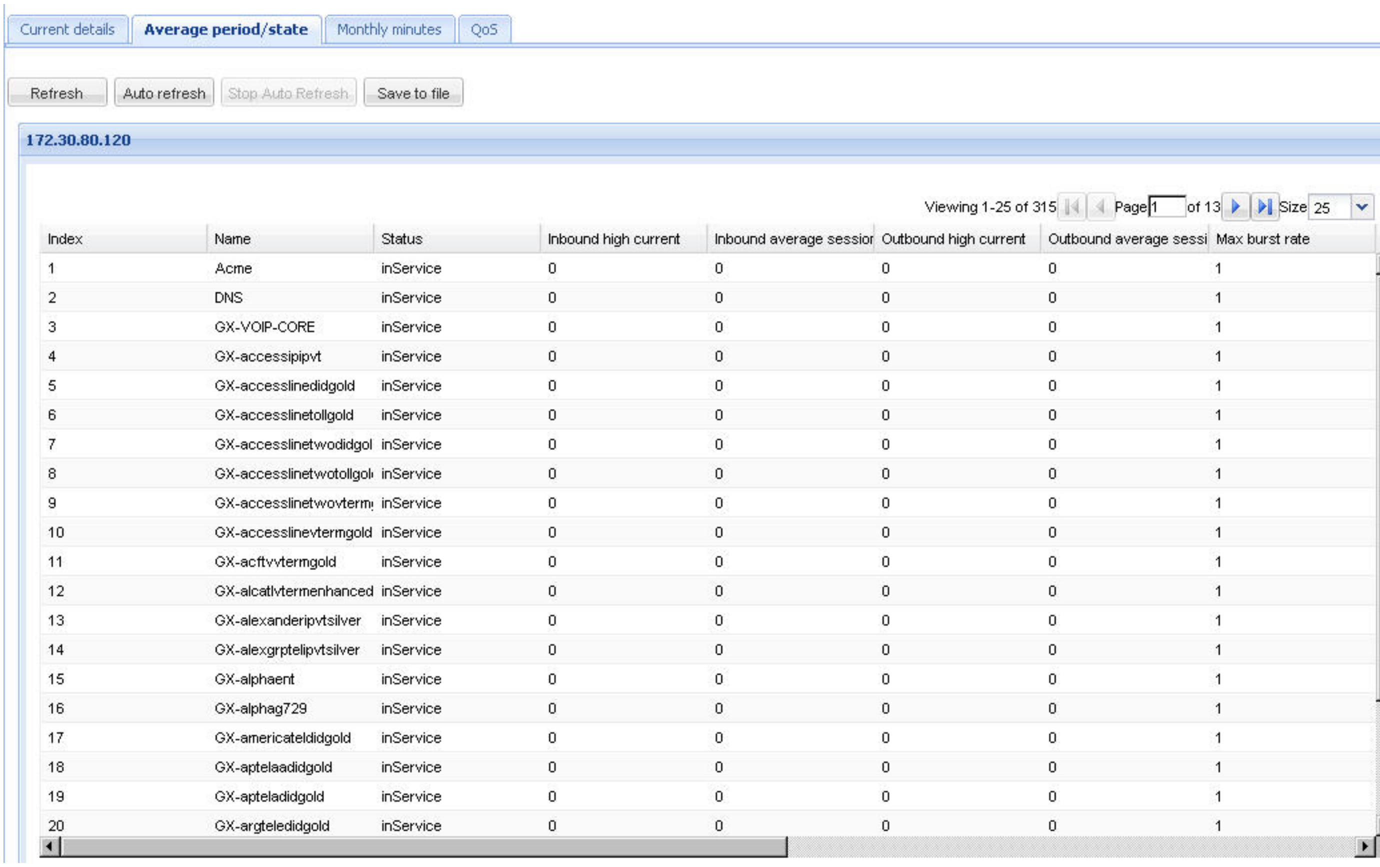
Data	Description
Index	A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1
Name	The name of the realm for which the following statistics are being calculated
Status	Current status of the specified realm, which is expressed as INS, constraintViolation, or callLoadReduction
Inbound	
Inbound active	Number of current active inbound sessions
Inbound active session rate	Current inbound session rate in CPS
Outbound	
Outbound active sessions	Number of current active outbound sessions
Outbound active session rate	Current outbound session rate in CPS
Period-based statistics	
Inbound	
Inbound admitted	Total number of inbound sessions during the period

Data	Description
Inbound not admitted	Total number of inbound sessions rejected due to insufficient bandwidth
Outbound	
Outbound admitted	Total number of outbound sessions during the period
Outbound not admitted	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

Average Period/State

To access average period/state data:

In the Realms window, click the Average period/state tab. The following data appears:



Index	Name	Status	Inbound high current	Inbound average sessior	Outbound high current	Outbound average sessi	Max burst rate
1	Acme	inService	0	0	0	0	1
2	DNS	inService	0	0	0	0	1
3	GX-VOIP-CORE	inService	0	0	0	0	1
4	GX-accessipipvt	inService	0	0	0	0	1
5	GX-accesslinedidgold	inService	0	0	0	0	1
6	GX-accesslinetollgold	inService	0	0	0	0	1
7	GX-accesslinetwodidgol	inService	0	0	0	0	1
8	GX-accesslinetwotollgol	inService	0	0	0	0	1
9	GX-accesslinetwovterm	inService	0	0	0	0	1
10	GX-accesslinevtermgold	inService	0	0	0	0	1
11	GX-acftvvtermgold	inService	0	0	0	0	1
12	GX-alcatlvtermenhanced	inService	0	0	0	0	1
13	GX-alexanderipvtsilver	inService	0	0	0	0	1
14	GX-alexgrptelipvtsilver	inService	0	0	0	0	1
15	GX-alphaent	inService	0	0	0	0	1
16	GX-alphag729	inService	0	0	0	0	1
17	GX-americateldidgold	inService	0	0	0	0	1
18	GX-aptelaadidgold	inService	0	0	0	0	1
19	GX-apteladidgold	inService	0	0	0	0	1
20	GX-argteledidgold	inService	0	0	0	0	1

The following table defines the information displayed:

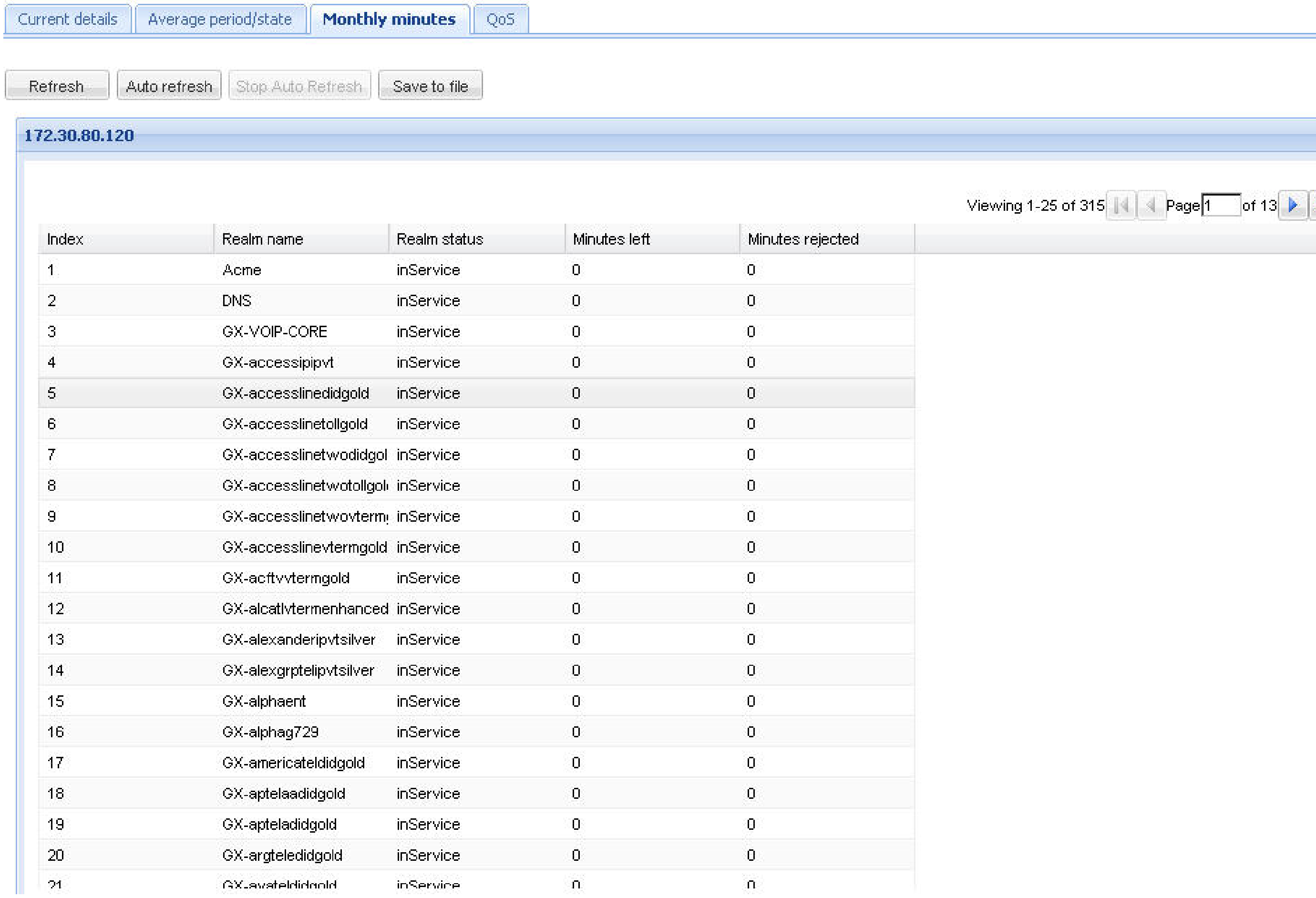
Data	Description
Index	A monotonically increasing integer for the sole purpose of indexing realms. When it reaches the maximum value the agent wraps the value back to 1
Name	The hostname of the realm for which the following statistics are being calculated
Status	The current status of the specified realm, which is expressed as INS, constraintsviolation, or callLoadReduction

Data	Description
Period-based statistics	
Inbound	
Inbound high current	Highest number of concurrent inbound sessions during the period
Inbound average session rate	Average rate of inbound sessions during the period in CPS
Outbound	
Outbound high current	Highest number of concurrent outbound sessions during the period
Outbound average session rate	Average rate of outbound sessions during the period in CPS
Period-based statistics	
Max burst rate	Maximum burst rate of traffic measured during the period (combined inbound and outbound)
Total seizures	Total number of seizures during the period
Total answered sessions	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	Average observed one-way signaling latency during the period in milliseconds
Max latency	Maximum observed one-way signaling latency during the period in milliseconds

Monthly Minutes

To access monthly minutes data:

In the Realms window, click the Monthly minutes tab. The following data appears:



Index	Realm name	Realm status	Minutes left	Minutes rejected
1	Acme	inService	0	0
2	DNS	inService	0	0
3	GX-VOIP-CORE	inService	0	0
4	GX-accessipipvt	inService	0	0
5	GX-accesslinedidgold	inService	0	0
6	GX-accesslinetollgold	inService	0	0
7	GX-accesslinetwodidgol	inService	0	0
8	GX-accesslinetwotollgol	inService	0	0
9	GX-accesslinetwovterm	inService	0	0
10	GX-accesslinevtermgold	inService	0	0
11	GX-acftvvtermgold	inService	0	0
12	GX-alcatlvtermenhanced	inService	0	0
13	GX-alexanderipvtsilver	inService	0	0
14	GX-alexgrptelipvtsilver	inService	0	0
15	GX-alphaent	inService	0	0
16	GX-alphag729	inService	0	0
17	GX-americateldidgold	inService	0	0
18	GX-aptelaadidgold	inService	0	0
19	GX-apteladidgold	inService	0	0
20	GX-argteledidgold	inService	0	0
21	GX-avateldidgold	inService	0	0

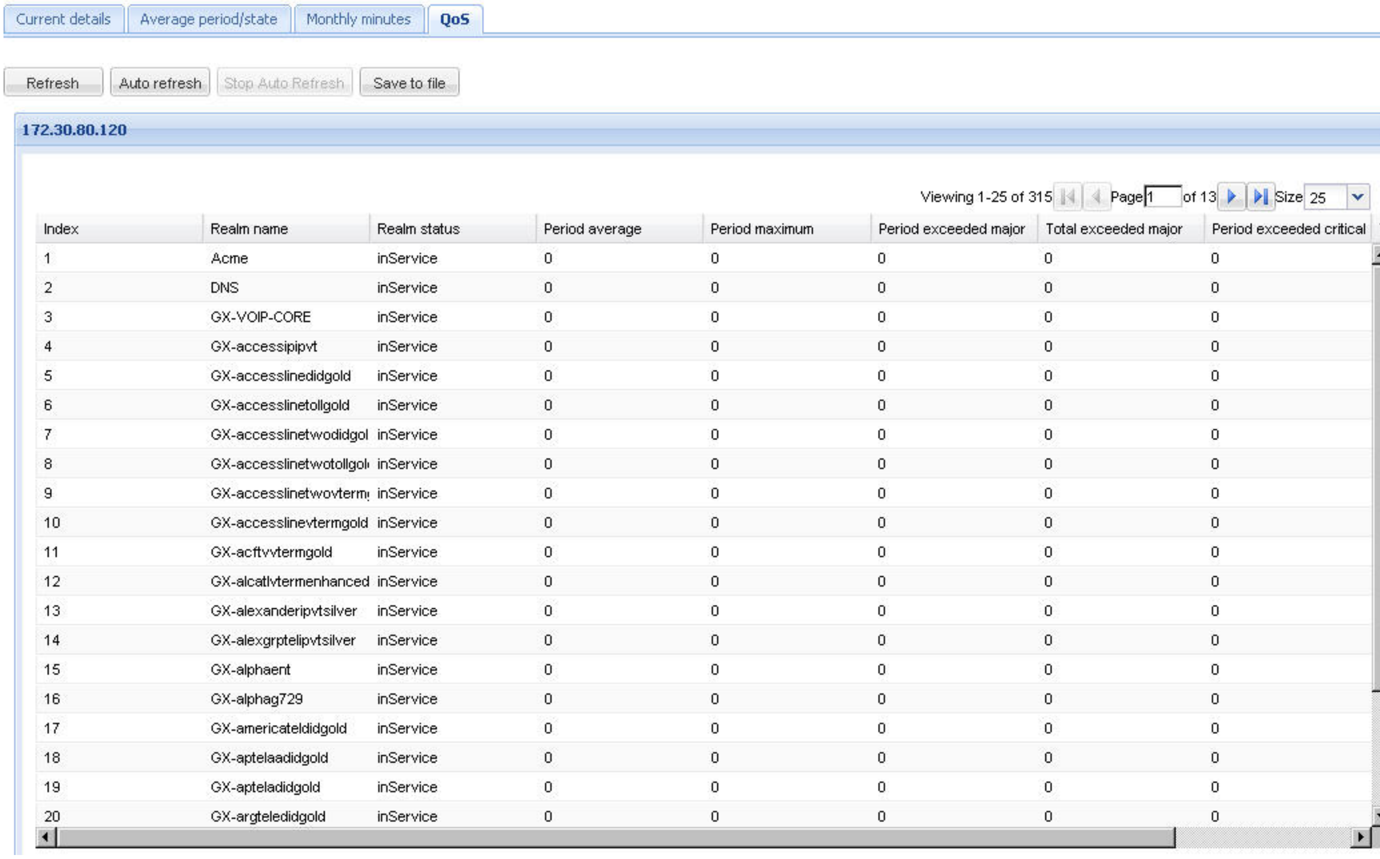
The following table defines the information displayed:

Data	Description
Index	A monotonically 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

QoS

To access QoS data:

In the Realms window, click the QoS tab. The following data appears:



Index	Realm name	Realm status	Period average	Period maximum	Period exceeded major	Total exceeded major	Period exceeded critical
1	Acme	inService	0	0	0	0	0
2	DNS	inService	0	0	0	0	0
3	GX-VOIP-CORE	inService	0	0	0	0	0
4	GX-accessipipvt	inService	0	0	0	0	0
5	GX-accesslinedidgold	inService	0	0	0	0	0
6	GX-accesslinetollgold	inService	0	0	0	0	0
7	GX-accesslinetwodidgol	inService	0	0	0	0	0
8	GX-accesslinetwotollgol	inService	0	0	0	0	0
9	GX-accesslinetwovterm	inService	0	0	0	0	0
10	GX-accesslinevtermgold	inService	0	0	0	0	0
11	GX-acftvvtermgold	inService	0	0	0	0	0
12	GX-alcatlvtermenhanced	inService	0	0	0	0	0
13	GX-alexanderipvtsilver	inService	0	0	0	0	0
14	GX-alexgrptelipvtsilver	inService	0	0	0	0	0
15	GX-alphaent	inService	0	0	0	0	0
16	GX-alphag729	inService	0	0	0	0	0
17	GX-americateldidgold	inService	0	0	0	0	0
18	GX-aptelaadidgold	inService	0	0	0	0	0
19	GX-apteladidgold	inService	0	0	0	0	0
20	GX-argteledidgold	inService	0	0	0	0	0

The following table defines the information displayed:

Data	Description
Index	A monotonically 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
Period-based statistics	
Period average	Average QoS factor observed during the period
Period maximum	Maximum QoS factor observed during the period
Period exceeded major	Peg counts the number of times the major Rfactor threshold was exceeded during the period
Total exceeded major	Peg counts the number of times the major Rfactor threshold was exceeded during the lifetime
Period exceeded critical	Peg counts the number of times the critical Rfactor threshold was exceeded during the period
Total exceeded critical	Peg counts the number of times the critical Rfactor threshold was exceeded during the lifetime

SIP Session

This section describes the SIP session data displayed by Oracle Communications Session Delivery Manager.

Accessing SIP Session Data

To access SIP session data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view SIP session data.
3. Click View. The list of performance data appears.
4. Click SIP session under the Performance Groups folder.

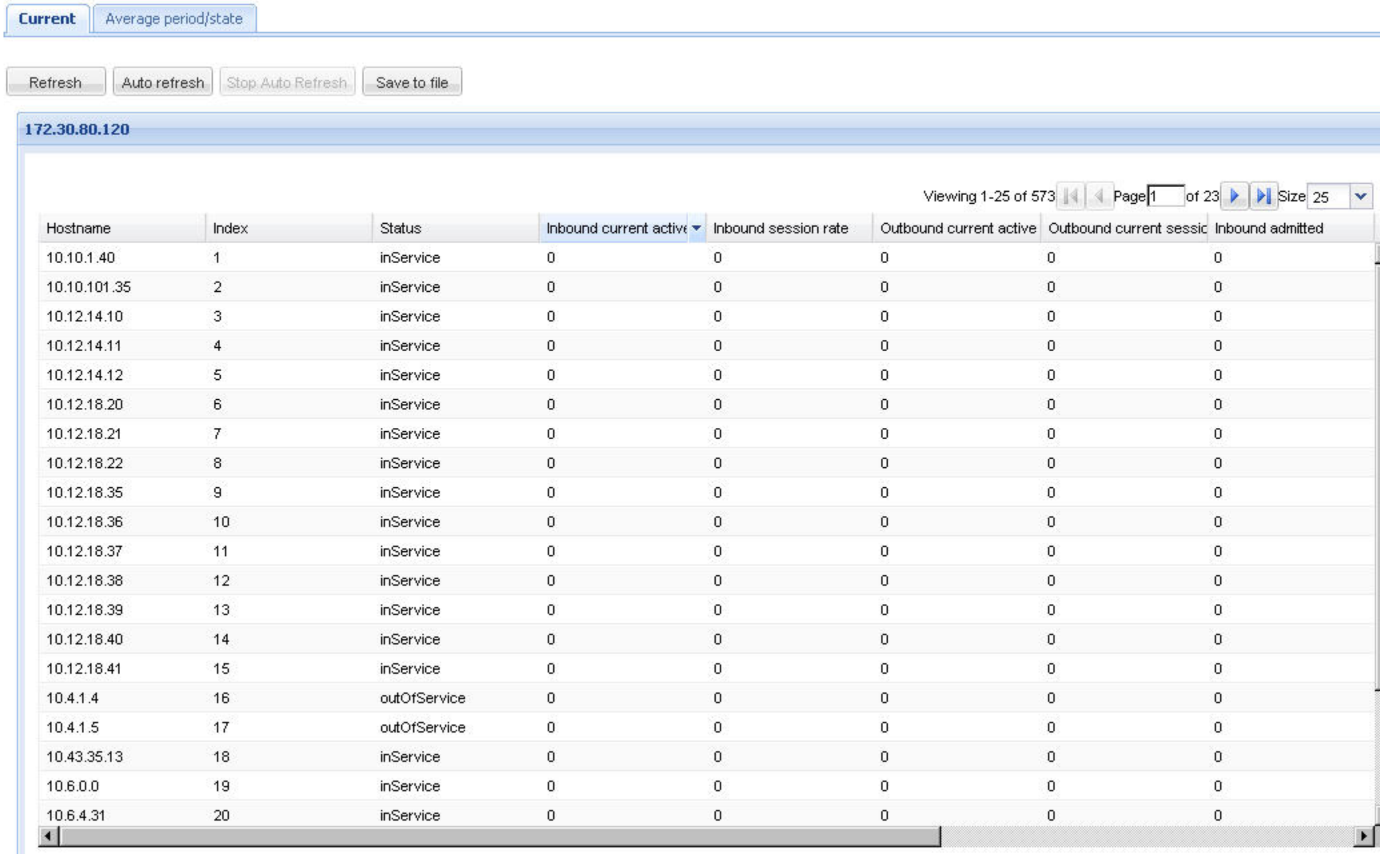
   The SIP session data appears for the following categories:

   - Current
   - Average period/state

Current

To access current data:

In the SIP session window, click the Current tab. The following data appears:



172.30.80.120

Viewing 1-25 of 573 Page 1 of 23 Size 25

Hostname	Index	Status	Inbound current active	Inbound session rate	Outbound current active	Outbound current sessic	Inbound admitted
10.10.1.40	1	inService	0	0	0	0	0
10.10.101.35	2	inService	0	0	0	0	0
10.12.14.10	3	inService	0	0	0	0	0
10.12.14.11	4	inService	0	0	0	0	0
10.12.14.12	5	inService	0	0	0	0	0
10.12.18.20	6	inService	0	0	0	0	0
10.12.18.21	7	inService	0	0	0	0	0
10.12.18.22	8	inService	0	0	0	0	0
10.12.18.35	9	inService	0	0	0	0	0
10.12.18.36	10	inService	0	0	0	0	0
10.12.18.37	11	inService	0	0	0	0	0
10.12.18.38	12	inService	0	0	0	0	0
10.12.18.39	13	inService	0	0	0	0	0
10.12.18.40	14	inService	0	0	0	0	0
10.12.18.41	15	inService	0	0	0	0	0
10.4.1.4	16	outOfService	0	0	0	0	0
10.4.1.5	17	outOfService	0	0	0	0	0
10.43.35.13	18	inService	0	0	0	0	0
10.6.0.0	19	inService	0	0	0	0	0
10.6.4.31	20	inService	0	0	0	0	0

The following table defines the information displayed:

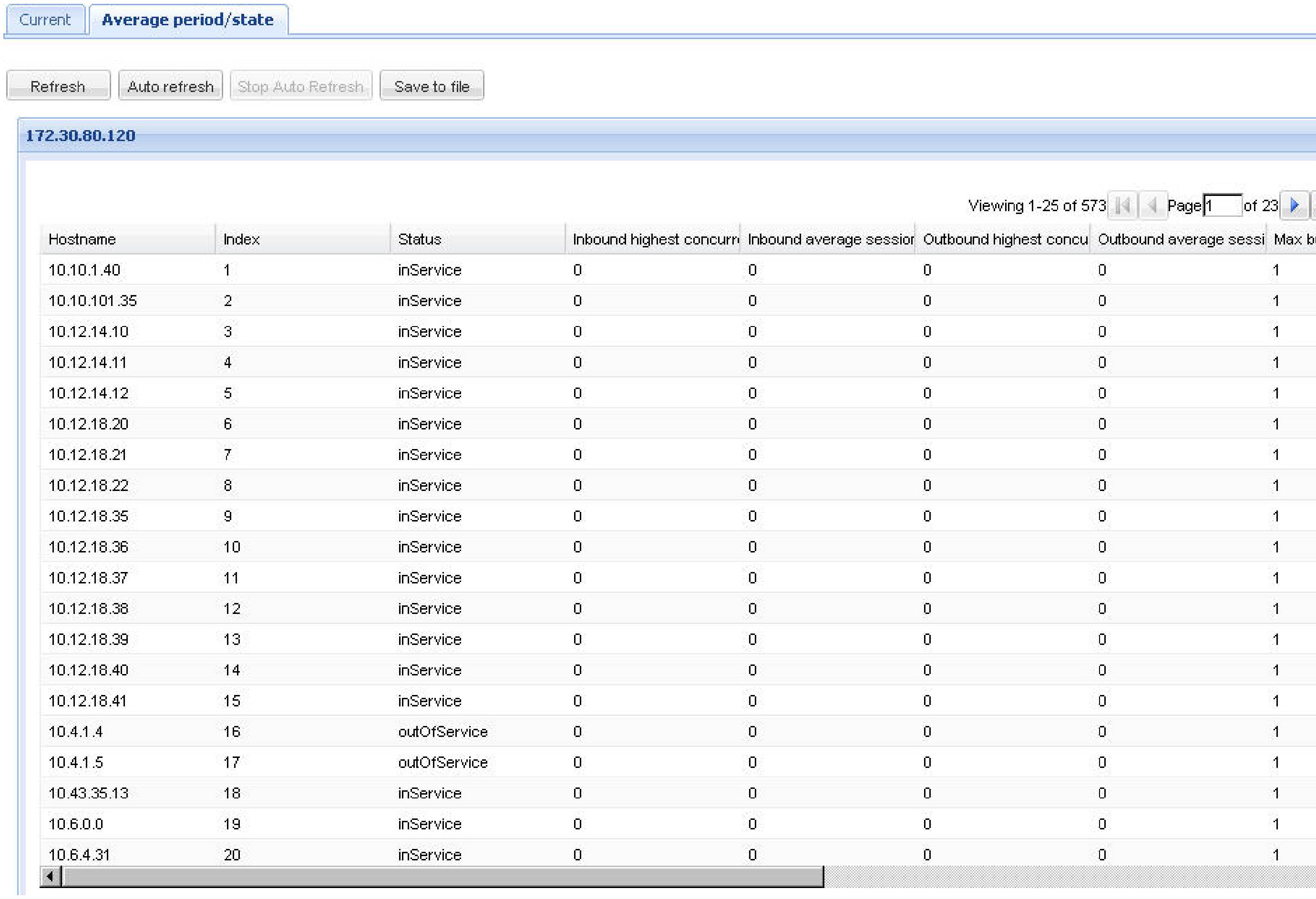
Data	Description
Hostname	The hostname of the session agent for which the following statistics are being calculated

Data	Description
Index	A monotonically increasing integer for the sole purpose of indexing 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	
Inbound current active sessions	Number of current active inbound sessions
Inbound current session rate	Current inbound session rate in CPS
Outbound	
Outbound current active sessions	Number of current active outbound sessions
Outbound current session rate	Current outbound session rate in CPS
Period-based statistics	
Inbound	
Inbound admitted	Total number of inbound sessions during the period
Inbound not admitted	Total number of inbound sessions rejected due to insufficient bandwidth
Outbound	
Outbound admitted	Total number of outbound sessions during the period
Outbound not admitted	Total number of outbound sessions rejected because of insufficient bandwidth

Average Period/State

To access current data:

In the SIP session window, click the Average period/state tab. The following data appears:



Hostname	Index	Status	Inbound highest concurr	Inbound average sessior	Outbound highest concu	Outbound average sessi	Max bu
10.10.1.40	1	inService	0	0	0	0	1
10.10.101.35	2	inService	0	0	0	0	1
10.12.14.10	3	inService	0	0	0	0	1
10.12.14.11	4	inService	0	0	0	0	1
10.12.14.12	5	inService	0	0	0	0	1
10.12.18.20	6	inService	0	0	0	0	1
10.12.18.21	7	inService	0	0	0	0	1
10.12.18.22	8	inService	0	0	0	0	1
10.12.18.35	9	inService	0	0	0	0	1
10.12.18.36	10	inService	0	0	0	0	1
10.12.18.37	11	inService	0	0	0	0	1
10.12.18.38	12	inService	0	0	0	0	1
10.12.18.39	13	inService	0	0	0	0	1
10.12.18.40	14	inService	0	0	0	0	1
10.12.18.41	15	inService	0	0	0	0	1
10.4.1.4	16	outOfService	0	0	0	0	1
10.4.1.5	17	outOfService	0	0	0	0	1
10.43.35.13	18	inService	0	0	0	0	1
10.6.0.0	19	inService	0	0	0	0	1
10.6.4.31	20	inService	0	0	0	0	1

The following table defines the information displayed:

Data	Description
Hostname	The hostname of the session agent for which the following statistics are being calculated
Index	A monotonically increasing integer for the sole purpose of indexing 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
Period-based statistics	
Inbound	
Inbound highest concurrent	Highest number of concurrent inbound sessions during the period
Inbound average session rate	Average rate of inbound sessions during the period in CPS

Data	Description
Outbound	
Outbound highest concurrent	Highest number of concurrent outbound sessions during the period
Outbound average session rate	Average rate of outbound sessions during the period in CPS
Period-based statistics	
Max burst rate	Maximum burst rate of traffic measured during the period (combined inbound and outbound)
Total seizures	Total number of seizures during the period
Total answered	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)	Average observed one-way signaling latency during the period
Maximum one-way signaling latency (ms)	Maximum observed one-way signaling latency during the period

H.323 Session

This section describes the H.323 session data displayed by Oracle Communications Session Delivery Manager.

Accessing H.323Session Data

To access H.323 session data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view H.323 session data.
3. Click View. The list of performance data appears.
4. Click H323 session under the Performance Groups folder.

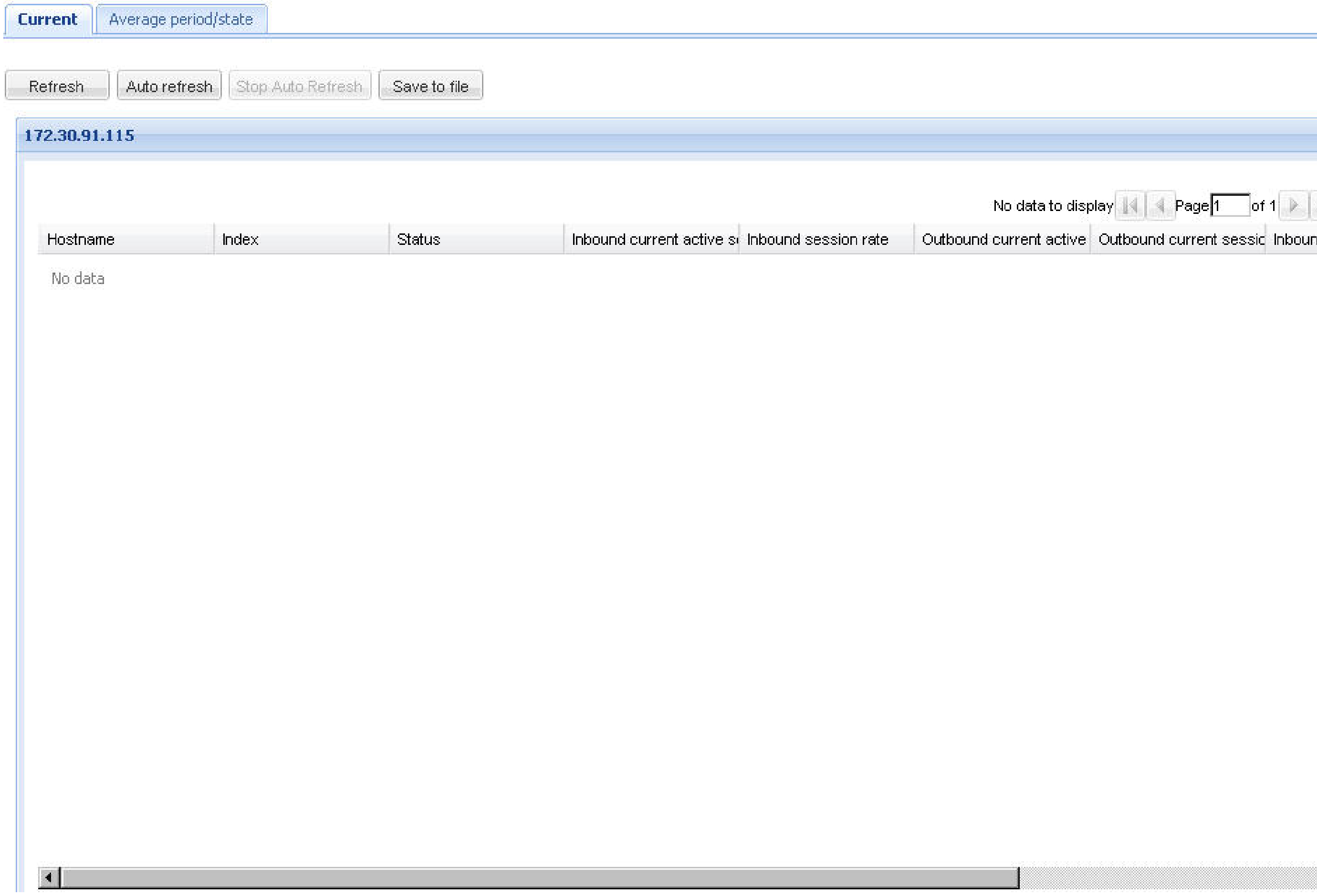
   The H.323 session data appears for the following categories:

   - Current
   - Average period/state

Current

To access H.323 session current data:

In the H323 session window, click the Current tab. The following data appears:



No data indicates there is no performance data for this performance category for this device.

The following table defines the information displayed:

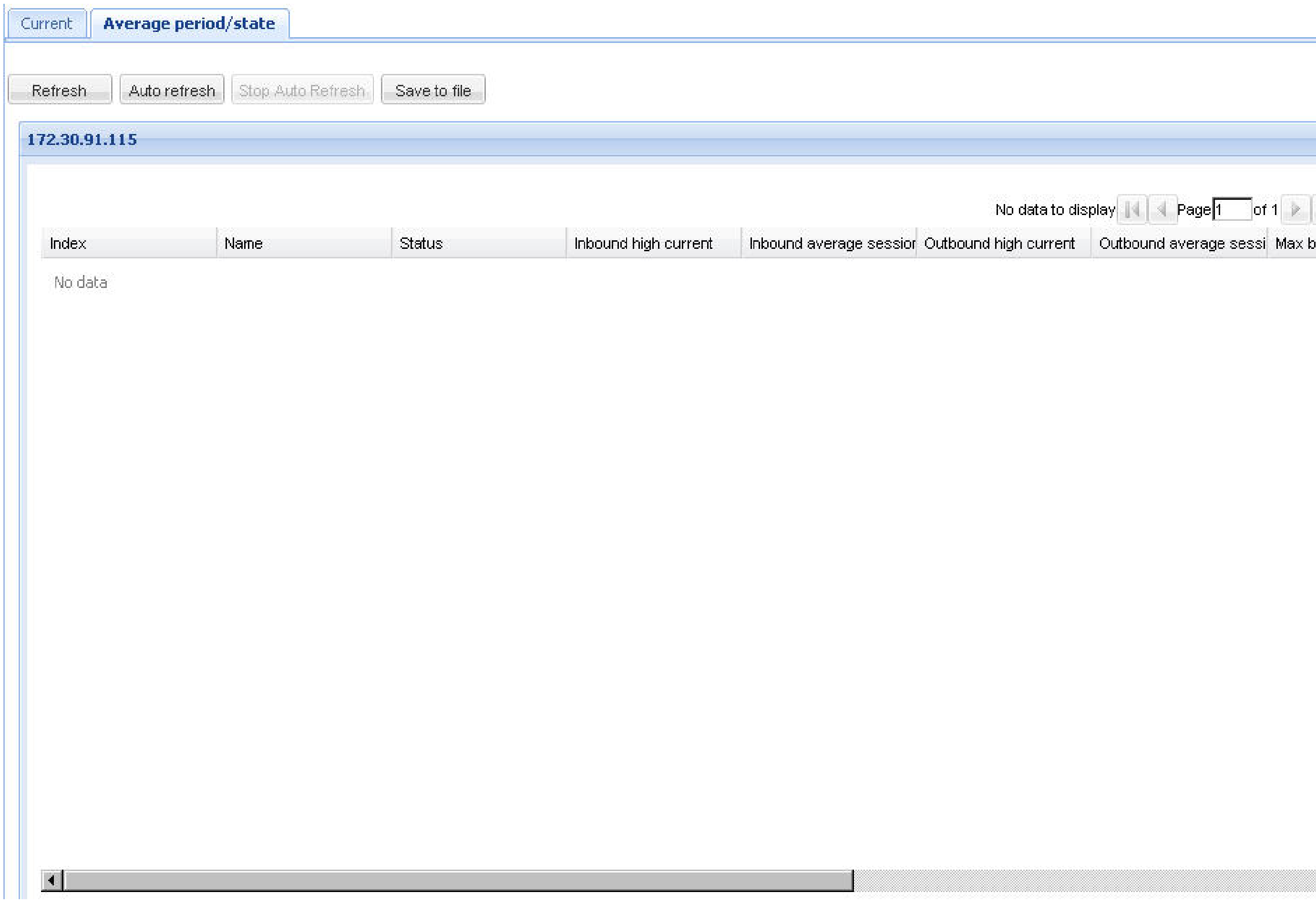
Data	Description
Hostname	The hostname of the session agent for which the statistics are being calculated
Index	A monotonically increasing integer for the sole purpose of indexing session agents. When it reaches the maximum value the agent wraps the value back to 1
Status	The current status of the specified session agent, which is expressed as: inService outOfService outOfServiceconstraintsviolation BecomingoutOfService ForcedoutOfService
Inbound	
Inbound current active sessions	Number of current active inbound sessions
Inbound session rate	Current Inbound Session rate in CPS

Data	Description
Outbound	
Outbound current active	Number of current active outbound sessions
Outbound current session rate	Current outbound session rate in CPS
Period-based statistics	
Inbound	
Inbound admitted	Total number of inbound sessions during the period
Inbound not admitted	Total number of inbound sessions rejected due to insufficient bandwidth
Outbound	
Outbound admitted	Total number of outbound sessions during the period
Outbound not admitted	Total number of outbound sessions rejected because of insufficient bandwidth

Average Period/State

To access H.323 session average period/state data:

In the H323 session window, click the Average period/state tab. The following data appears:



Index	Name	Status	Inbound high current	Inbound average sessior	Outbound high current	Outbound average sessi	Max b
No data							

The following table defines the information displayed:

Data	Description
Index	A monotonically increasing integer for the sole purpose of indexing session agents. 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
Status	The current status of the specified session agent, which is expressed as: inService outOfService outOfServiceconstraintsviolation BecomingoutOfService ForcedoutOfService
Period-based statistics	
Inbound	
Inbound high current	Highest number of concurrent inbound sessions during the period
Inbound average session rate	Average rate of inbound sessions during the period in CPS
Outbound	
Outbound high current	Highest number of concurrent outbound sessions during the period
Outbound average session rate	Average rate of outbound sessions during the period in CPS
Period-based statistics	
Max burst rate	Maximum burst rate of traffic measured during the period (combined inbound and outbound)
Total seizures	Total number of seizures during the period
Total answered	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	Average observed one-way signaling latency during the period
Max latency	Maximum observed one-way signaling latency during the period

Codec

This section describes the codec data displayed by Oracle Communications Session Delivery Manager.

Note: Codec data is available for D-series Net-Net SBCs only.

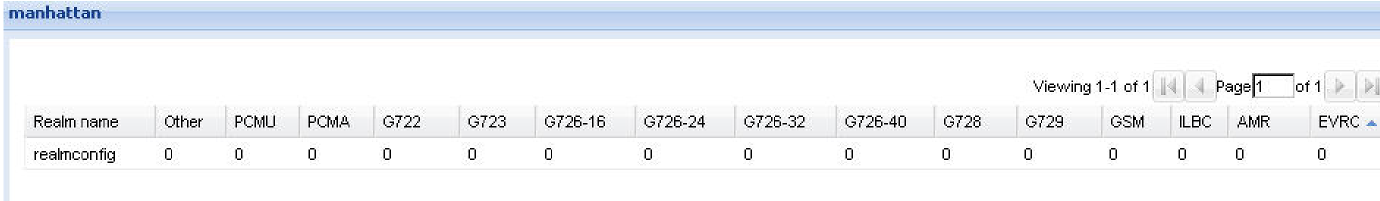
Accessing Codec Data

To access codec data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view codec data.
3. Click View. The list of performance data appears.

4. Click Codec under the Performance Groups folder.

   The Codec data appears.



Realm name	Other	PCMU	PCMA	G722	G723	G726-16	G726-24	G726-32	G726-40	G728	G729	GSM	ILBC	AMR	EVRC
realmconfig	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The following table defines the information displayed.

Data	Description
Realm	The realm that corresponds with the codec listed
Other	Other codecs not matched with the standard, well-known list of codecs
All standard, well-known codecs are listed in the remaining columns.	

Transcoding

This section describes the transcoding data displayed by Oracle Communications Session Delivery Manager.

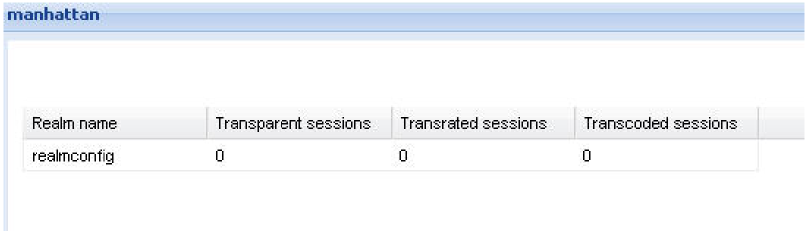
Note: Transcoding data is available for D-series Net-Net SBCs only.

Accessing Transcoding Data

To access transcoding data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view transcoding data.
3. Click View. The list of performance data appears.
4. Click Transcoding under the Performance Groups folder.

   The transcoding data appears.



Realm name	Transparent sessions	Transrated sessions	Transcoded sessions
realmconfig	0	0	0

The following table defines the information displayed.

Data	Description
Realm name	The name of the realm for which the following statistics are being calculated
Transparent sessions	Counts of sessions that require no TCU hardware intervention (all end-to-end media uses the same codec)
Transrated sessions	Counts of sessions that use the Net-Net SBC’s TCUs to change the packetization interval among dialogs in the session
Transcoded sessions	Counts of sessions that use the Net-Net SBC’s TCUs to transcode between two or more codecs

NSEP

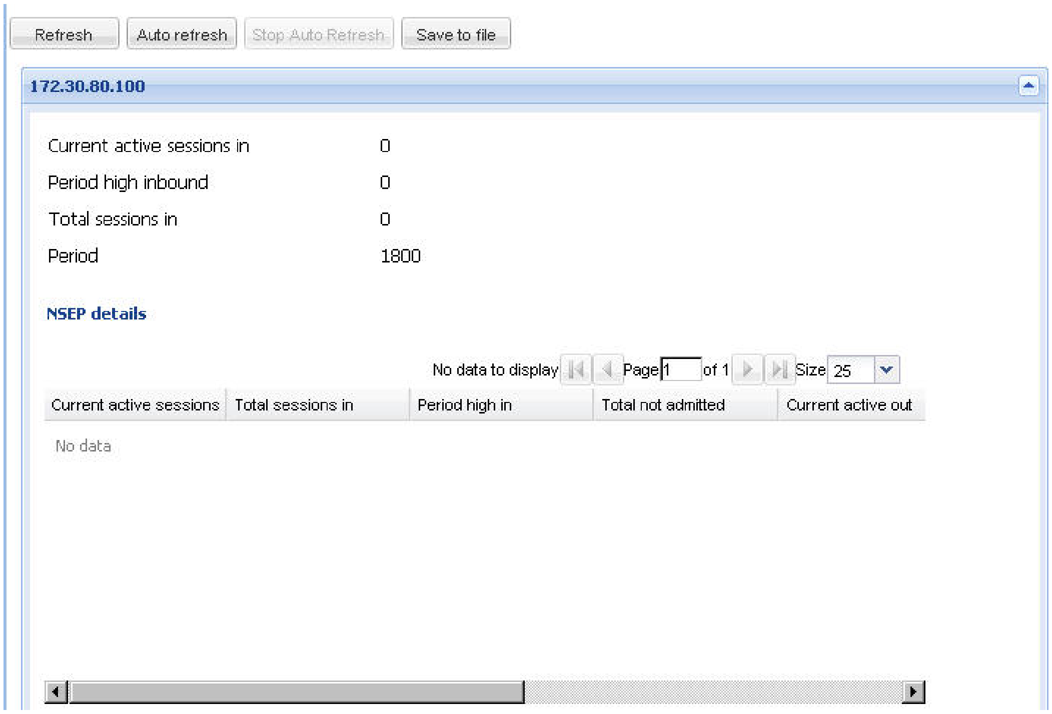
This section describes the NSEP data displayed by Oracle Communications Session Delivery Manager.

Accessing NSEP Data

To access NSEP data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view NSEP data.
3. Click View. The list of performance data appears.
4. Click NSEP under the Performance Groups folder.

   The NSEP data appears.



Current active sessions in 0

Period high inbound 0

Total sessions in 0

Period 1800

NSEP details

No data to display Page 1 of 1 Size 25

Current active sessions	Total sessions in	Period high in	Total not admitted	Current active out
No data				

The following table defines the information displayed:

Data	Description
Current active sessions in	Number of current active inbound NSEP sessions
Period high inbound	Highest number of concurrent inbound NSEP sessions during the period
Total sessions in	Total number of inbound NSEP sessions during the period
Period	The period for which the statistics are collected in seconds
NSEP details	
Inbound	
Current active sessions in	Number of current active NSEP sessions
Total sessions in	Total number of inbound NSEP sessions during the period

Data	Description
Period high in	Highest number of concurrent inbound NSEP sessions during the period
Total not admitted	Total number of inbound NSEP sessions rejected
Outbound	
Current active out	Number of current active outbound NSEP sessions
Total sessions out	Total number of outbound NSEP sessions during the period
Period high out	Highest number of concurrent outbound NSEP sessions during the period
Total not admitted	Total number of outbound NSEP sessions rejected

Trap Table Summary

This section describes the summary of trap data generated by the Net-Net SBC.

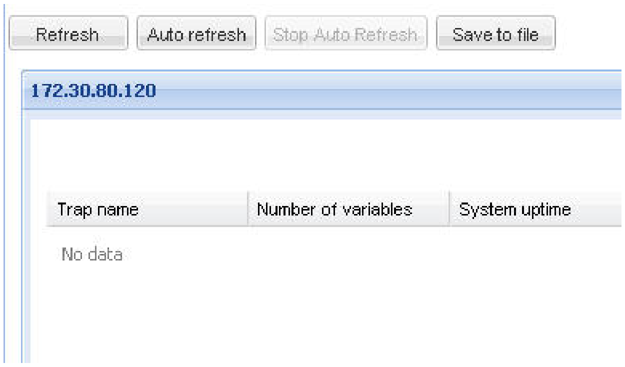
Note: Trap table summary data is available for the C-series Net-Net SBCs only.

Accessing Trap Table Summary Data

To access trap table summary data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view trap table summary data.
3. Click View. The list of performance data appears.
4. Click Trap table summary under the Performance Groups folder.

   The trap table data appear.



The following table defines the information displayed:

Data	Description
Trap name	Trap name for this fault condition
Number of variables	The number of variables encoded in the trap
System uptime	The snmp sysUptime when the trap was generated

Storage Utilization

This section describes the summary of storage utilization data generated by the Net-Net SBC.

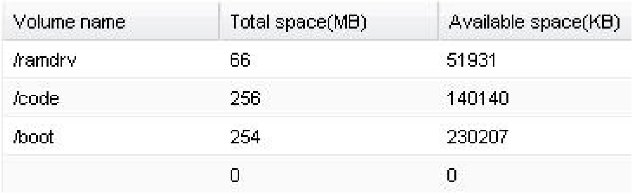
Note: Storage utilization data is available for the C-Series Net-Net SBCs only.

Accessing Storage Utilization Data

To access storage utilization data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view storage utilization data.
3. Click View. The list of performance data appears.
4. Click Storage utilization under the Performance Groups folder.

   The storage utilization data appear.



Volume name	Total space(MB)	Available space(KB)
/ramdrv	66	51931
/code	256	140140
/boot	254	230207
	0	0

The following table defines the information displayed:

Data	Description
Volume name	The name of the disk partition as defined by the user
Total space (MB)	Total amount of disk space
Available space (KB)	Available, free disk space available

Intrusion Detection System (IDS)

This section describes the intrusion detection system (IDS) data displayed by Oracle Communications Session Delivery Manager.

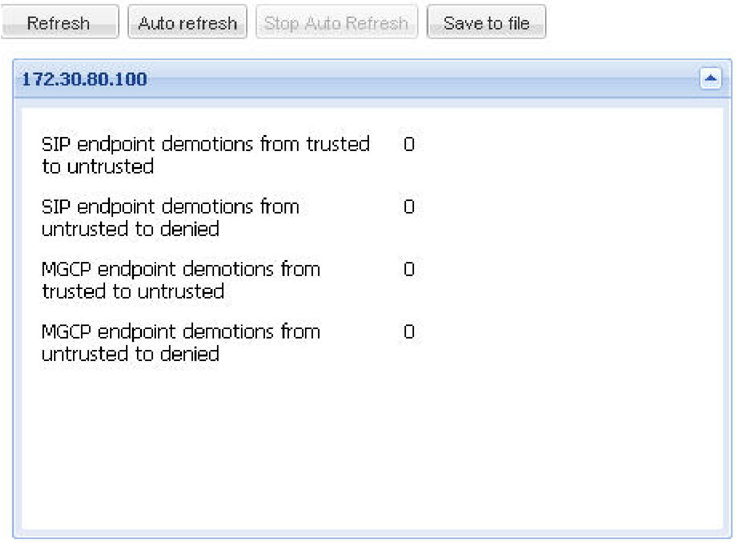
Note: IDS data is available for the C-series Net-Net SBCs only.

Accessing IDS Data

To access IDS data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view IDS data.
3. Click View. The list of performance data appears.
4. Click IDS under the Performance Groups folder.

   The IDS data appear.



SIP endpoint demotions from trusted to untrusted 0

SIP endpoint demotions from untrusted to denied 0

MGCP endpoint demotions from trusted to untrusted 0

MGCP endpoint demotions from untrusted to denied 0

The following table defines the information displayed:

Data	Description
SIP endpoint demotions from trusted to untrusted	Global counters for SIP endpoint demotions from trusted to untrusted
SIP endpoint demotions from untrusted to denied	Global counters for SIP endpoint demotions from untrusted to denied
MGCP endpoint demotions from trusted to untrusted	Global counter for MGCP endpoint demotions from trusted to untrusted
MGCP endpoint demotions from untrusted to denied	Global counters for MGCP endpoint demotions from untrusted to denied

Cached Contacts

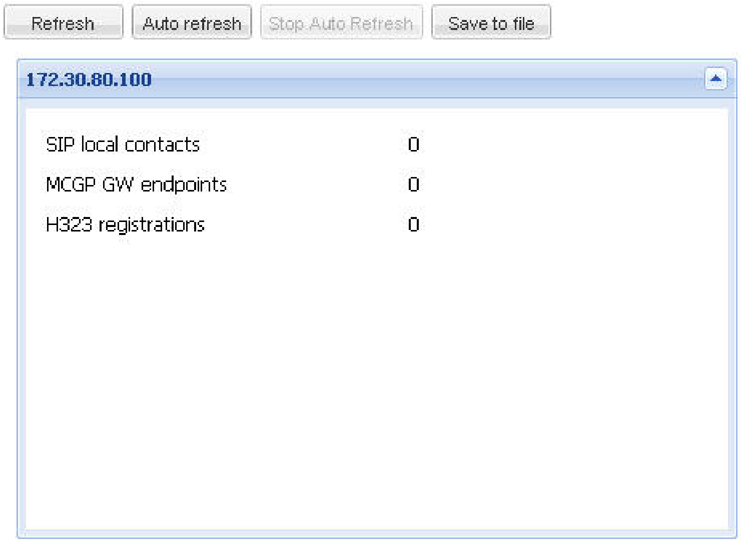
This section describes the number of cached contact data displayed by Oracle Communications Session Delivery Manager.

Accessing Cached Contacts Data

To access cached contacts data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view cached contacts data.
3. Click View. The list of performance data appears.
4. Click Cached contacts under the Performance Groups folder.

   The cached contact data appear.



172.30.80.100

SIP local contacts	0
MCGP GW endpoints	0
H323 registrations	0

The following table defines the information displayed:

Data	Description
SIP local contacts	Number of active SIP local contacts
MGCP GW endpoints	Number of MGCP GW endpoints
H.323 registrations	Number of H.323 registrations

Network Management Controls

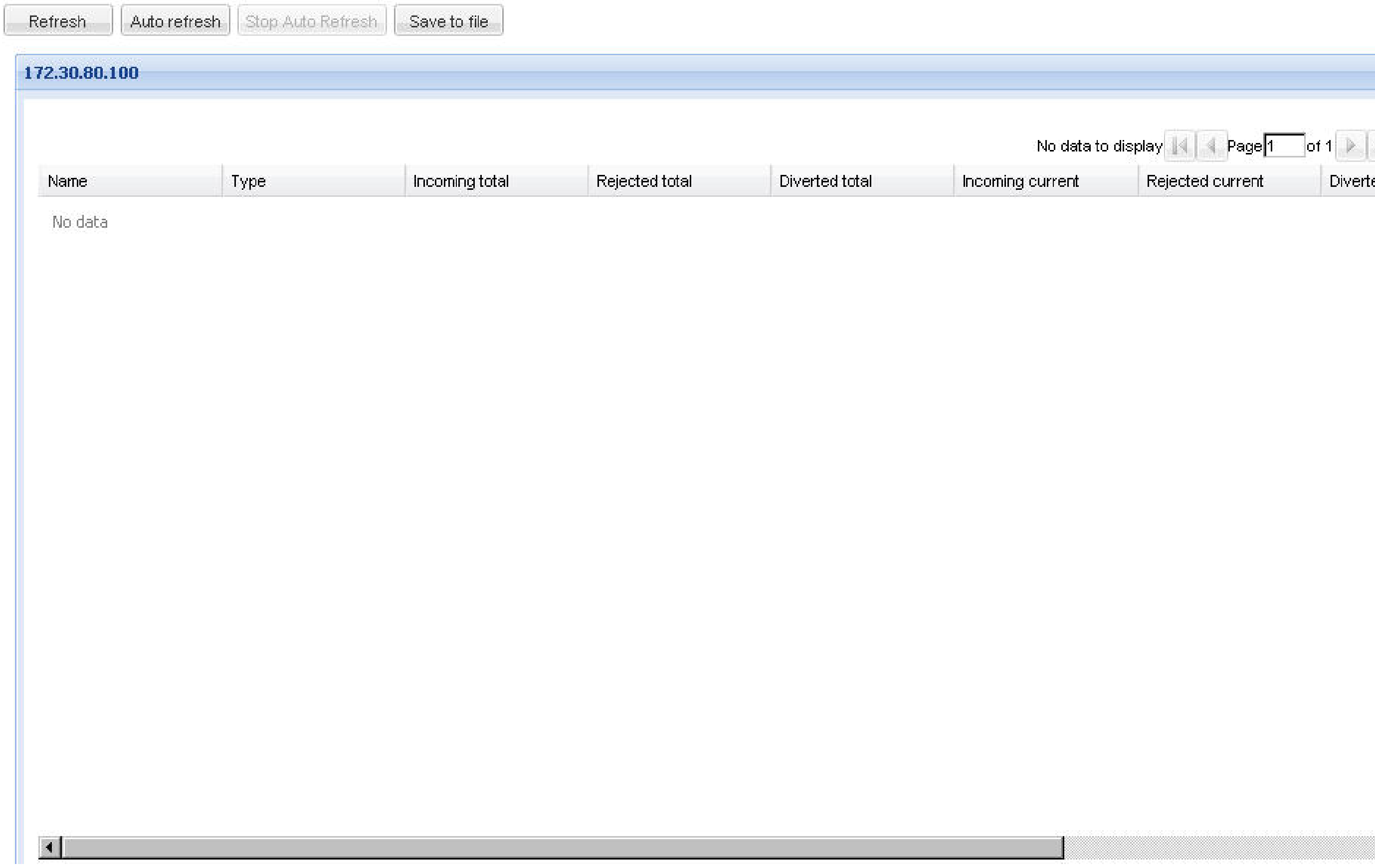
This section describes the network management (NM) control data displayed by Oracle Communications Session Delivery Manager.

Accessing NM Control Data

To access NM control data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view NM control performance data.
3. Click View. The list of performance data appears.
4. Click NM controls under the Performance Groups folder.

   The NM controls data appear.



No data

The following table defines the information displayed:

Data	Description
Name	Name of the network management control
Type	Type of network management control
Incoming total	Total number of incoming calls that match a destination identifier
Rejected total	Total number of incoming calls that are rejected
Diverted total	Total number of incoming calls that are diverted
Incoming current	Number of incoming calls during the current period that match a destination identifier
Rejected current	Number of incoming calls that are rejected during the current period
Diverted current	Number of incoming calls diverted during the current period
Incoming period max	Maximum number of incoming calls during a period that match a destination identifier
Rejected period max	Number of the maximum incoming calls rejected in a period
Diverted period max	Number of the maximum incoming calls diverted in a period

ENUM Servers

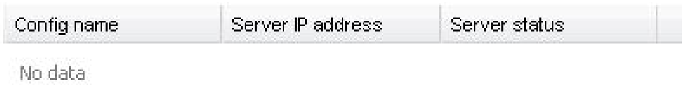
This section describes the ENUM server table data displayed by Oracle Communications Session Delivery Manager.

Accessing ENUM Servers Data

To access ENUM servers data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view ENUM servers data.
3. Click View. The list of performance data appears.
4. Click ENUM servers under the Performance Groups folder.

   The ENUM servers data appear.



Config name	Server IP address	Server status
No data		

The following table defines the information displayed:

Data	Description
Config name	Name of the ENUM configuration
Server IP address	IP address for the ENUM server
Server status	Status of the ENUM server

CPU Core Table

This section describes the CPU core table data displayed by Oracle Communications Session Delivery Manager.

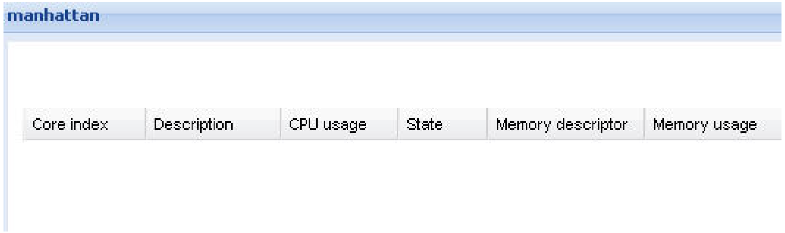
Note: CPU core table data is available for D-series Net-Net SBCs only.

Accessing CPU Core Table Data

To access CPU core table data:

1. Expand the Performance Manager slider and click Devices.
2. Click the device in the device table for which you want to view CPU core table data.
3. Click View. The list of performance data appears.
4. Click CPU core table under the Performance Groups folder.

   The CPU core table data appears.



manhattan

Core index	Description	CPU usage	State	Memory descriptor	Memory usage

If there is no data, the table is empty.

The following table defines the information displayed:

Data	Description
Core index	A monotonically increasing integer for the sole purpose of indexing
Description	Provides core ID and slot location
CPU usage	Percentage of total CPU being used
State	Indicates current state
Memory descriptor	Describes type of RAM memory
Memory usage	Indicates current RAM being used

7

Work Order Administration

Introduction

Work order administration allows you to perform software upgrades and global parameter changes across a targeted group of devices. You create a customized work order, assign your devices (also referred to as targeted devices), and execute it to apply the changes.

Note: Oracle Communications Session Delivery Manager does not support work order administration for certain configuration elements. Please consult the Known Issues table of the Oracle Communications Session Delivery Manager 7.3 Release Notes.

Work orders support two types of operations:

- Software upgrade: Allows you to automatically upgrade and downgrade the software version for multiple devices.
- Global parameter changes: Allows you to automatically provision multiple devices by changing configuration parameters.

A work order consists of:

- Work order type: 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 execution procedure (steps to be performed on the targeted devices) and is based on the type of work order you create: Software upgrade or global parameter changes.

About Work Order Administration

Predefined Work Flows

There is a predefined work flow process for each type of work order. A predefined work flow is the automated steps Oracle Communications Session Delivery Manager performs to complete the work order. Once you select the type of work order you want to execute and the targeted devices you want to update, Oracle Communications Session Delivery Manager processes these steps until your work order is completed. Refer to *Predefined Work Flows* for tables listing the steps and corresponding processes for all work order scenarios.

Each predefined work flow has a corresponding predefined rollback process in the event that a rollback to the previous state is necessary.

You cannot edit the predefined work flows.

Software Upgrade

If you are performing a software upgrade, you can manually execute the work order or set it to execute automatically at a set time. For example, you can configure Oracle Communications Session Delivery Manager to perform these upgrades during a maintenance window. Oracle Communications Session Delivery Manager then upgrades the targeted devices in your work order until the work order is completed.

Global Parameter Changes

If you are performing global parameter changes, first you must create a global configuration. The global configuration is comprised of elements and attributes seeded from one of two options: a managed device or a software version. Next, you load your global configuration. The global configuration stores all of the changes made during configuration. Finally, you create the work order, select targeted devices, associate the global configuration with the work order and execute it, or schedule it to execute.

Before You Start

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 Delivery Manager clusters. Please ensure SFTP servers are running for Oracle Communications Session Delivery 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 Delivery 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 Delivery 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 Delivery Manager Software image archive management table. If the targeted Oracle Communications Session Delivery Manager server is in a cluster, the Oracle Communications Session Delivery 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 Delivery 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.

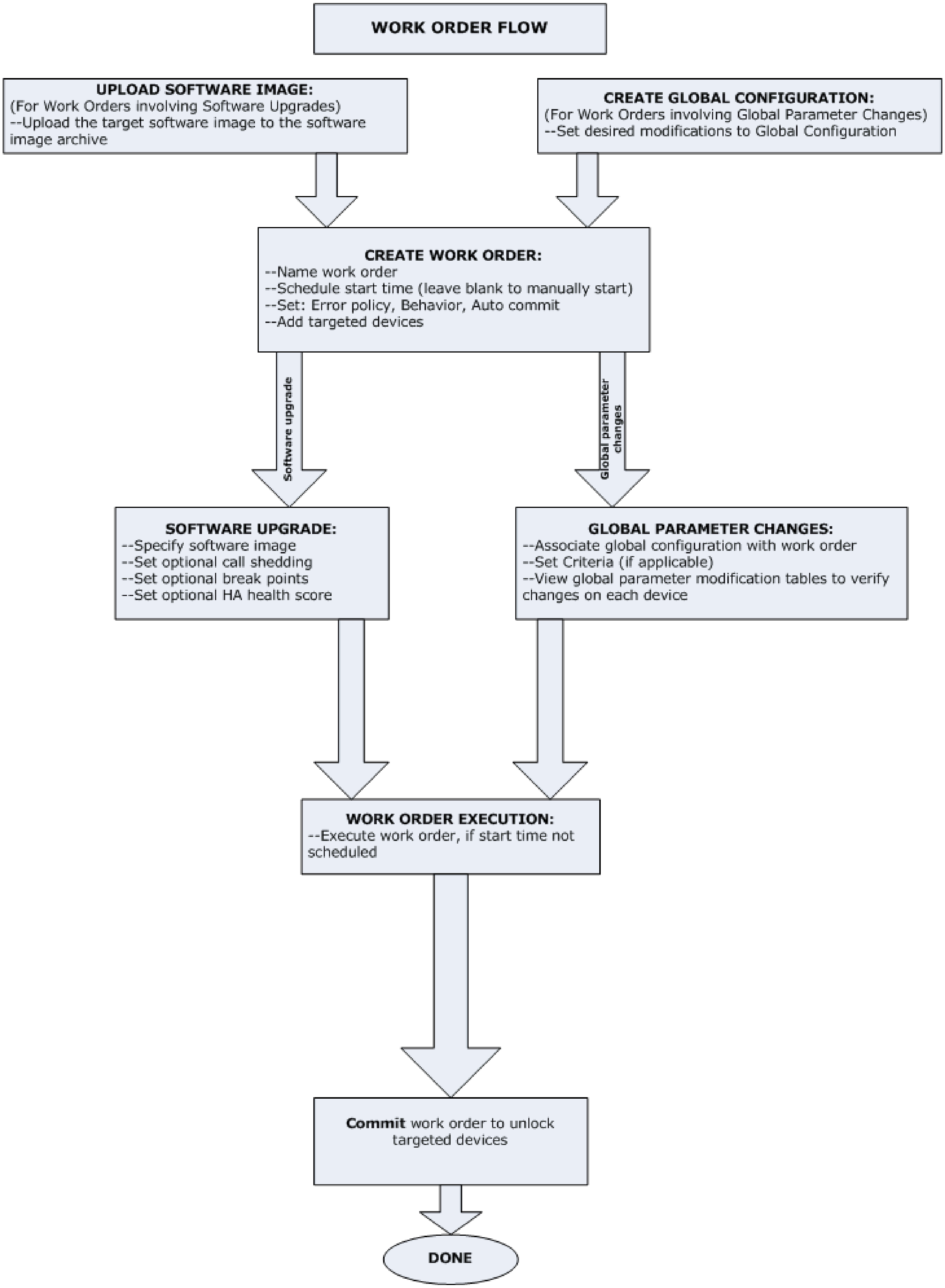
1. Upload the target software image to the software image archive. Refer to *Adding Software Images to the Software Image Archive Directory* for more information.
2. Create a software upgrade work order. Refer to *Creating a Software Upgrade Work Order* for more information.
3. Name the work order.
4. 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 FLOW
UPLOAD SOFTWARE IMAGE:
(For Work Orders involving Software Upgrades)
--Upload the target software image to the software image archive
CREATE GLOBAL CONFIGURATION:
(For Work Orders involving Global Parameter Changes)
--Set desired modifications to Global Configuration
CREATE WORK ORDER:
--Name work order
--Schedule start time (leave blank to manually start)
--Set: Error policy, Behavior, Auto commit
--Add targeted devices
Software upgrade
Global parameter changes
SOFTWARE UPGRADE:
--Specify software image
--Set optional call shedding
--Set optional break points
--Set optional HA health score
GLOBAL PARAMETER CHANGES:
--Associate global configuration with work order
--Set Criteria (if applicable)
--View global parameter modification tables to verify changes on each device
WORK ORDER EXECUTION:
--Execute work order, if start time not scheduled
Commit work order to unlock targeted devices
DONE

Work Order Administration Graphical User Interface

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

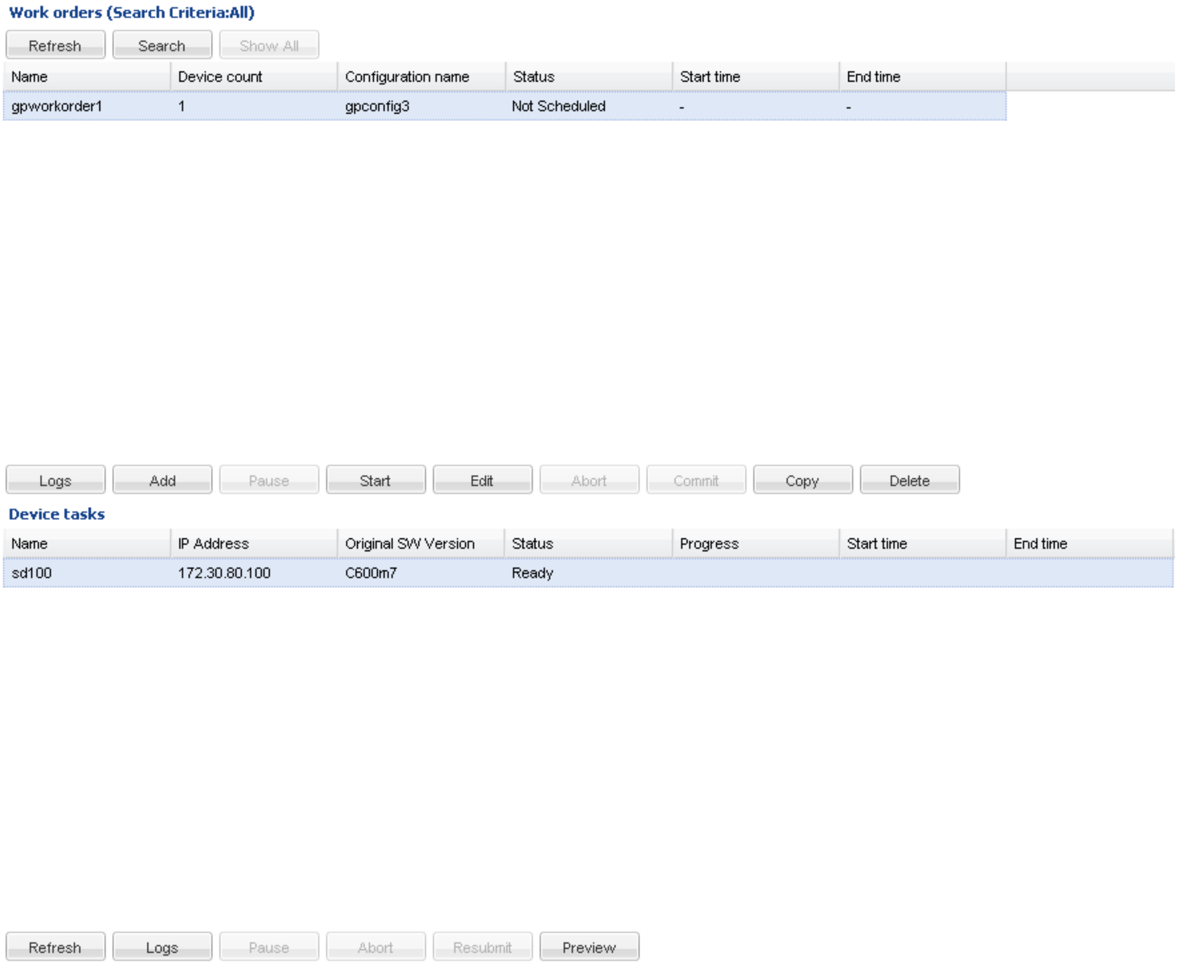
You access the software upgrade work order administration in the Device Manager slider. You access the global parameter changes work order administration in the Configuration Manager slider. Refer to the *Performing a Software Upgrade* or *Performing Global Parameter Changes* sections for instructions.

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.



Work orders (Search Criteria:All)

Name	Device count	Configuration name	Status	Start time	End time
gpworkorder1	1	gpconfig3	Not Scheduled	-	-

Device tasks

Name	IP Address	Original SW Version	Status	Progress	Start time	End time
sd100	172.30.80.100	C600m7	Ready			

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 Delivery 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 Delivery Manager database. The Oracle Communications Session Delivery 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.

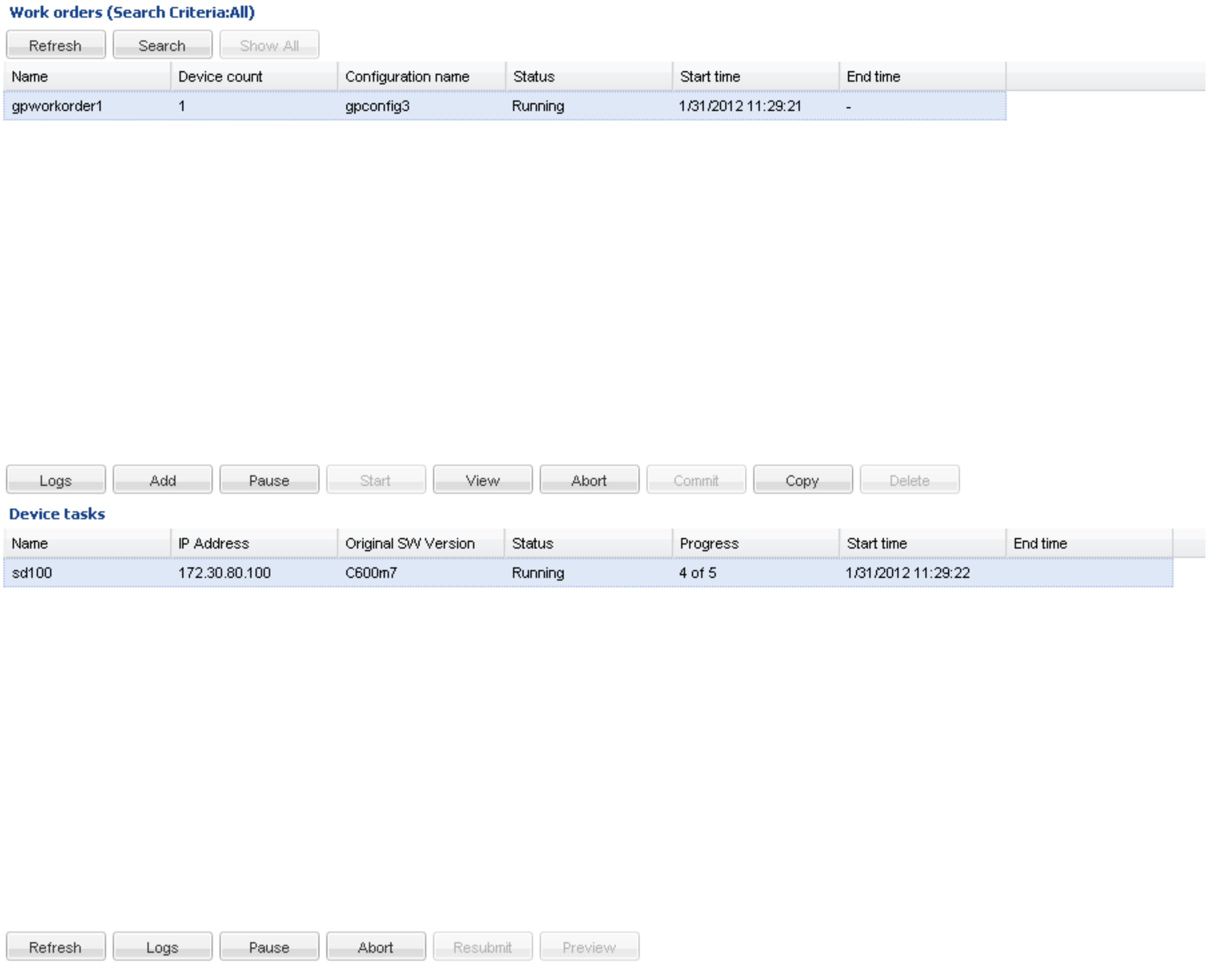
Data	Description
Configuration Name	For global parameter changes only: Global configuration name applied in this work order.
Target SW version	For software upgrades only: The software version to be installed.
Status	The possible statuses of the work order: PartiallyConfigured: Configuration is incomplete. 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 Delivery 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.

Data	Description
	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 Delivery Manager server start date and local time for this work order.
End time	The end time is the Oracle Communications Session Delivery 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.



Name	Device count	Configuration name	Status	Start time	End time
gpworkorder1	1	gpconfig3	Running	1/31/2012 11:29:21	-

Name	IP Address	Original SW Version	Status	Progress	Start time	End time
sd100	172.30.80.100	C600m7	Running	4 of 5	1/31/2012 11:29:22	

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 Delivery 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.
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.

Data	Description
Start time	Oracle Communications Session Delivery 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 Delivery 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.

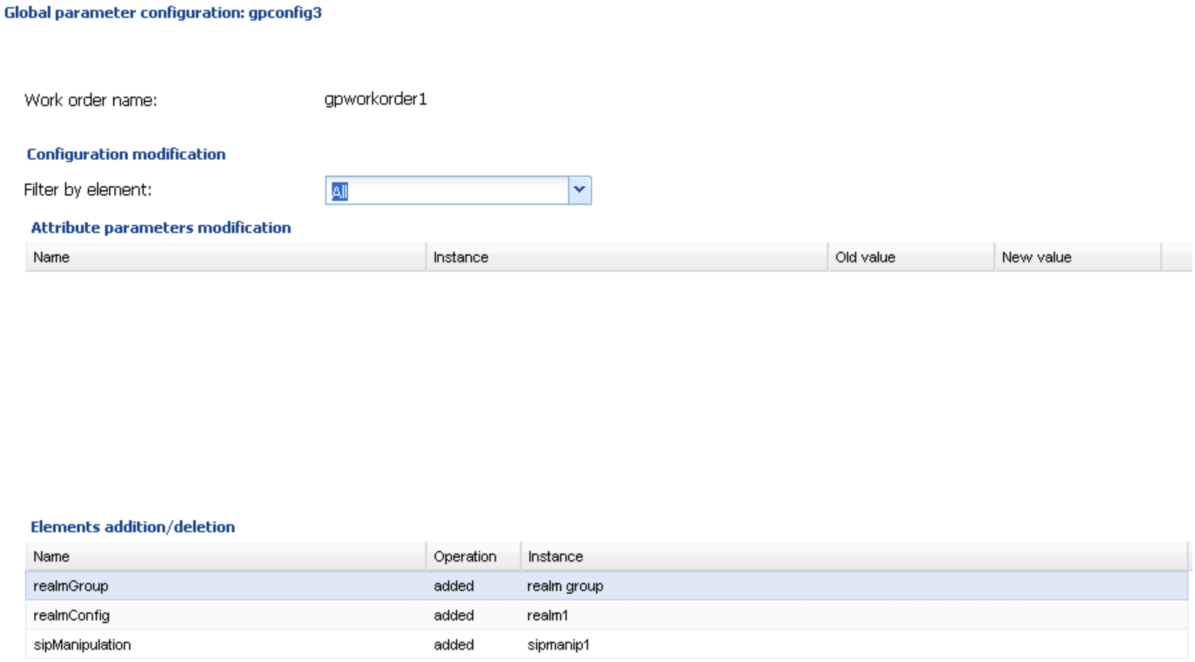
Configuration and Attributes Modification Tables

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.



Global parameter configuration: gpconfig3

Work order name: gpworkorder1

Configuration modification

Filter by element: All

Attribute parameters modification

Name	Instance	Old value	New value

Elements addition/deletion

Name	Operation	Instance
realmGroup	added	realm group
realmConfig	added	realm1
sipManipulation	added	sipmanip1

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.

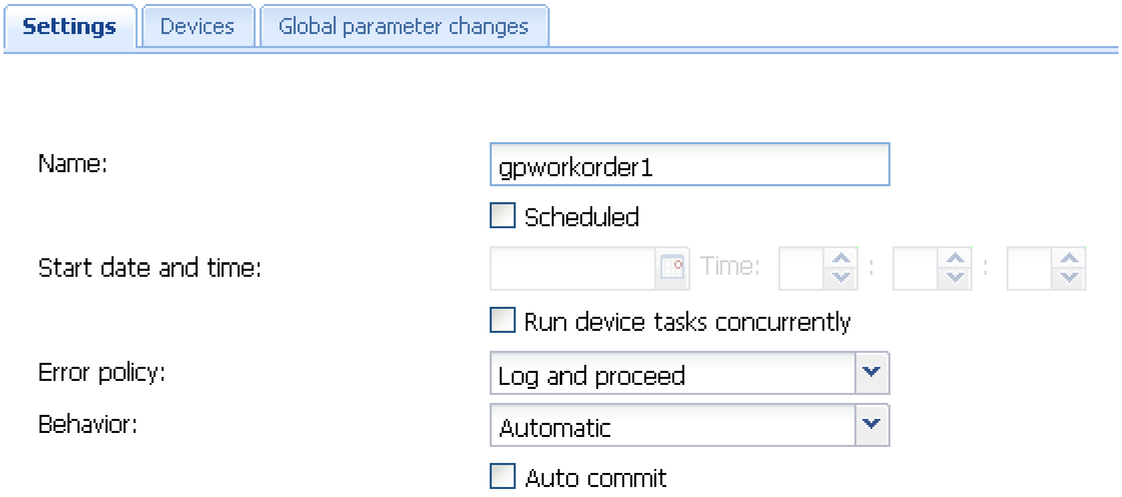
Data	Description
Name	The name of the element type which is going to be added or deleted.
Instance	String value of the key to identify the specific element instance.
Operation	Operation performed on this element: Add: This element was added to this global configuration. Delete: This element was deleted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



Name: gpworkorder1

□ Scheduled

Start date and time: Time: : :

□ Run device tasks concurrently

Error policy: Log and proceed

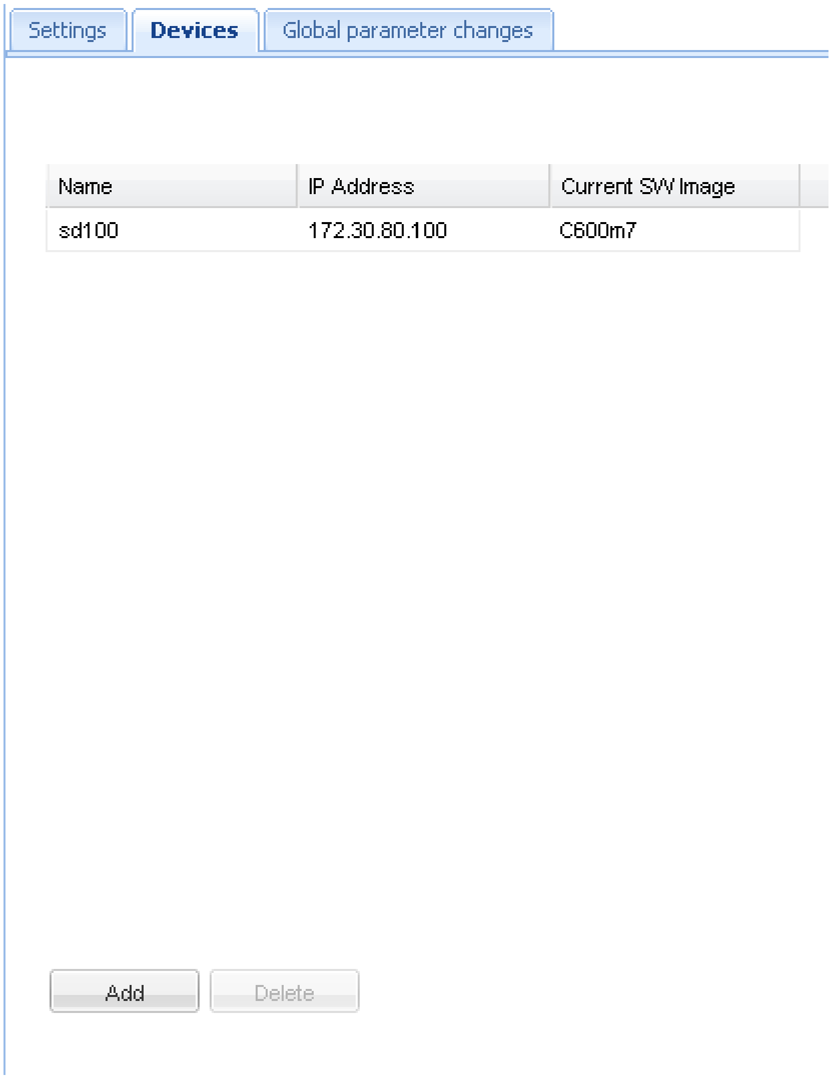
Behavior: Automatic

□ Auto commit

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

Devices Tab

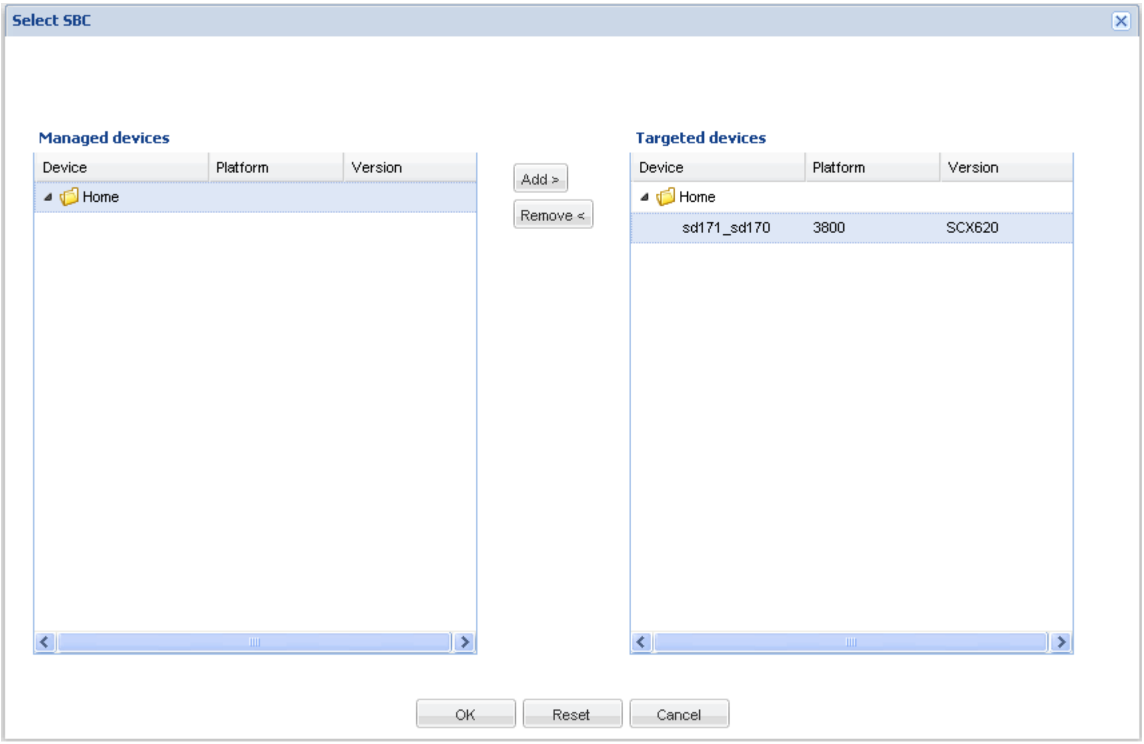
The Devices tab allows you to select targeted devices for your work order.



Name	IP Address	Current SW Image
sd100	172.30.80.100	C600m7

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.

- 

Managed devices

Device	Platform	Version
Home		

Targeted devices

Device	Platform	Version
Home		
sd171_sd170	3800	SCX620

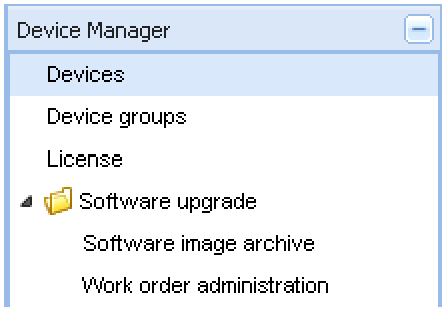
For more information on configuring these parameters, please consult the *Adding Targeted Devices* section.

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.

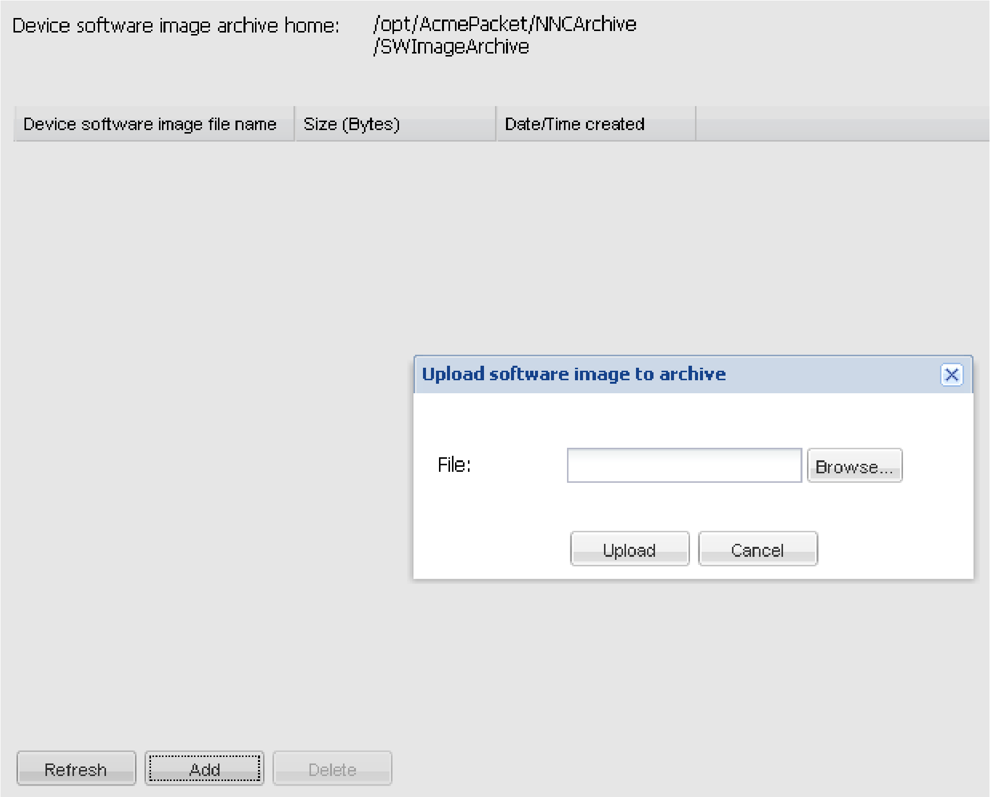


Software Image Archive

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*.



Device software image archive home: /opt/AcmePacket/NNCArchive/SWImageArchive

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

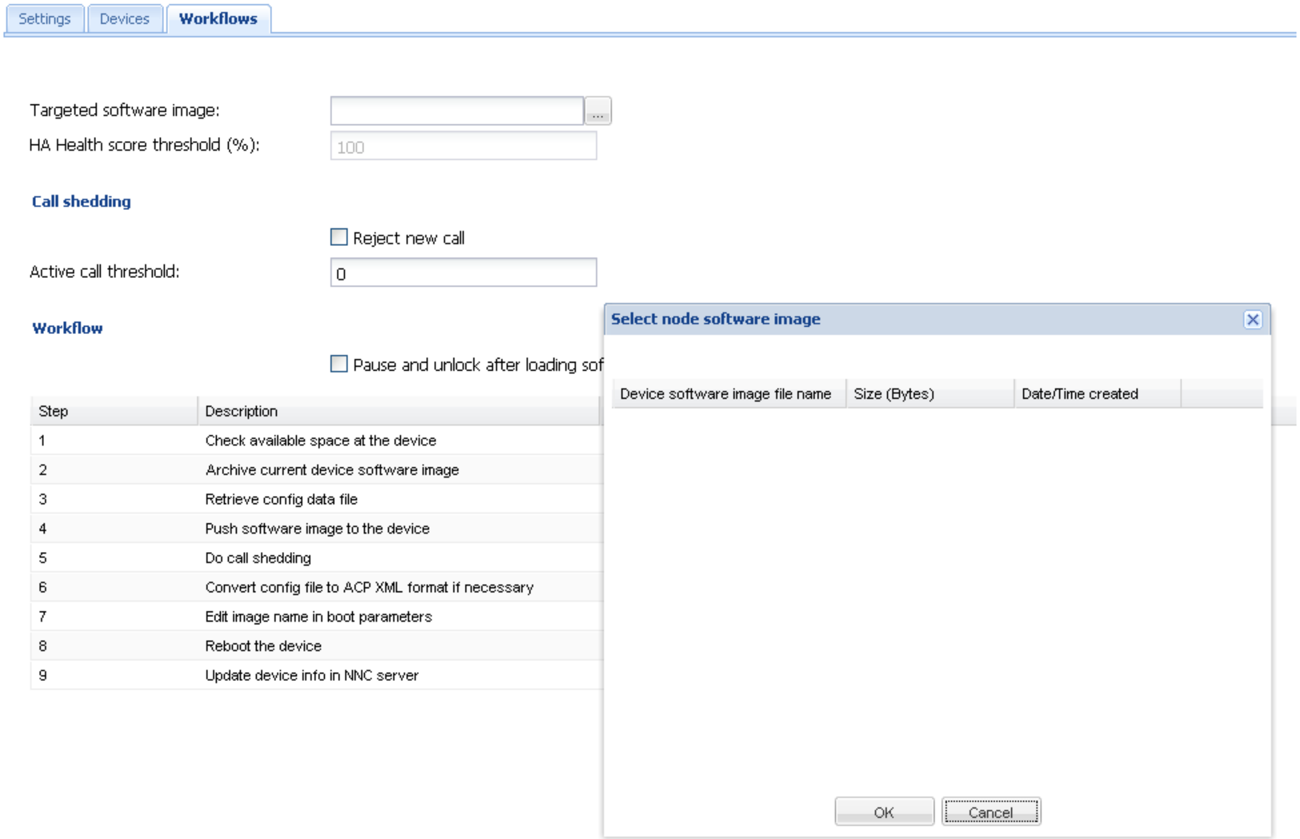
The software archive management action buttons allow you to:

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*.



Targeted software image:

HA Health score threshold (%): 100

Call shedding

□ Reject new call

Active call threshold: 0

Workflow

□ Pause and unlock after loading sof

Step	Description
1	Check available space at the device
2	Archive current device software image
3	Retrieve config data file
4	Push software image to the device
5	Do call shedding
6	Convert config file to ACP XML format if necessary
7	Edit image name in boot parameters
8	Reboot the device
9	Update device info in NNC server

Select node software image

Device software image file name	Size (Bytes)	Date/Time created

Global Parameter Changes Work Order Administration

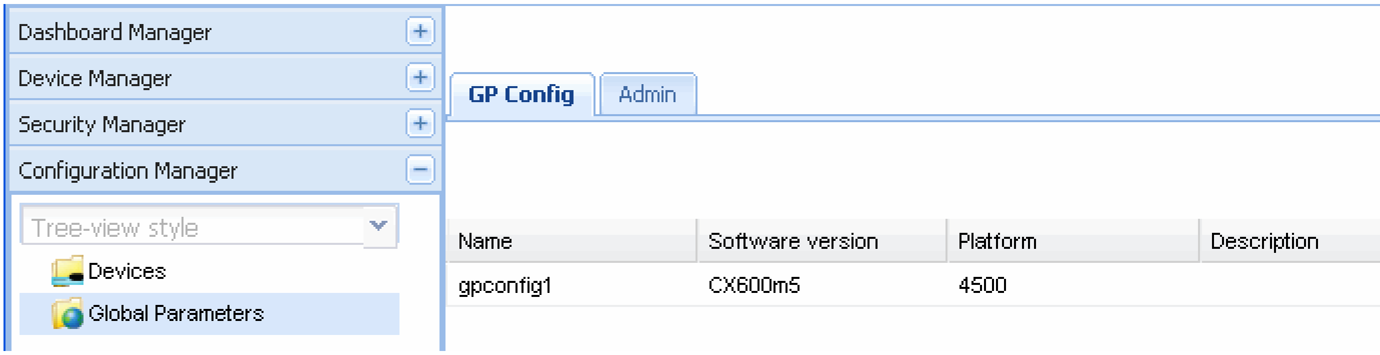
Now we will discuss elements that are unique to global parameter changes work orders. Before you create a global parameter changes work order, you must create a global configuration to store your configuration modifications.

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.



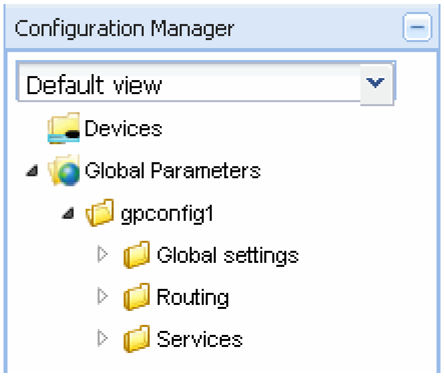
Name	Software version	Platform	Description
gpconfig1	CX600m5	4500	

Loading a Global Configuration

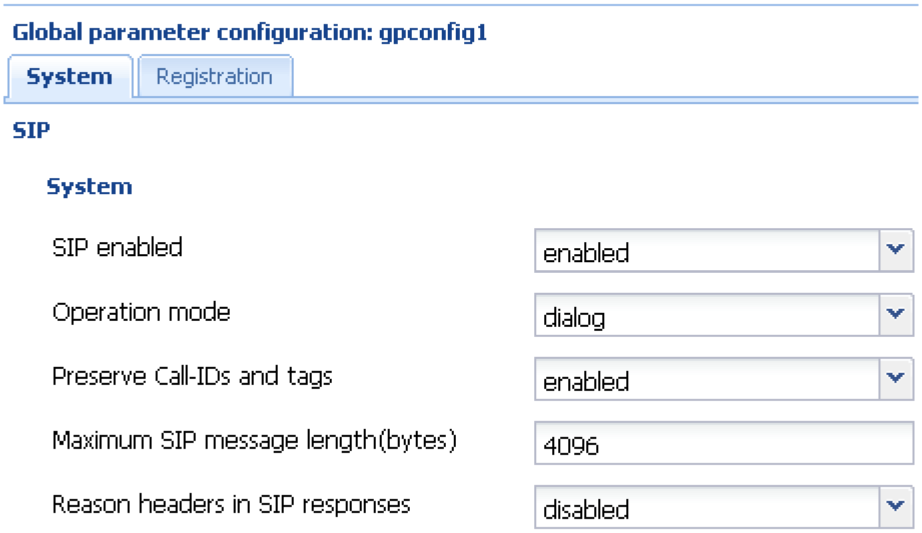
To load a global configuration:

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.



SIP enabled	enabled
Operation mode	dialog
Preserve Call-IDs and tags	enabled
Maximum SIP message length(bytes)	4096
Reason headers in SIP responses	disabled

GP Config Tab Actions

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

Action	Description
Refresh	Net-NetCentral 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.
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.

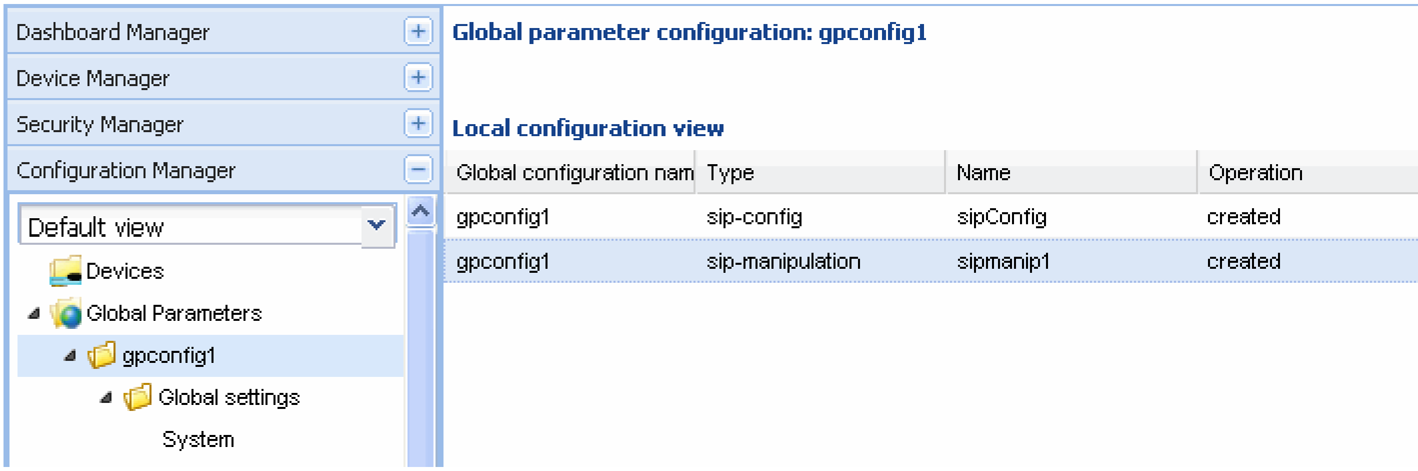
GP Config Tab Data

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*.



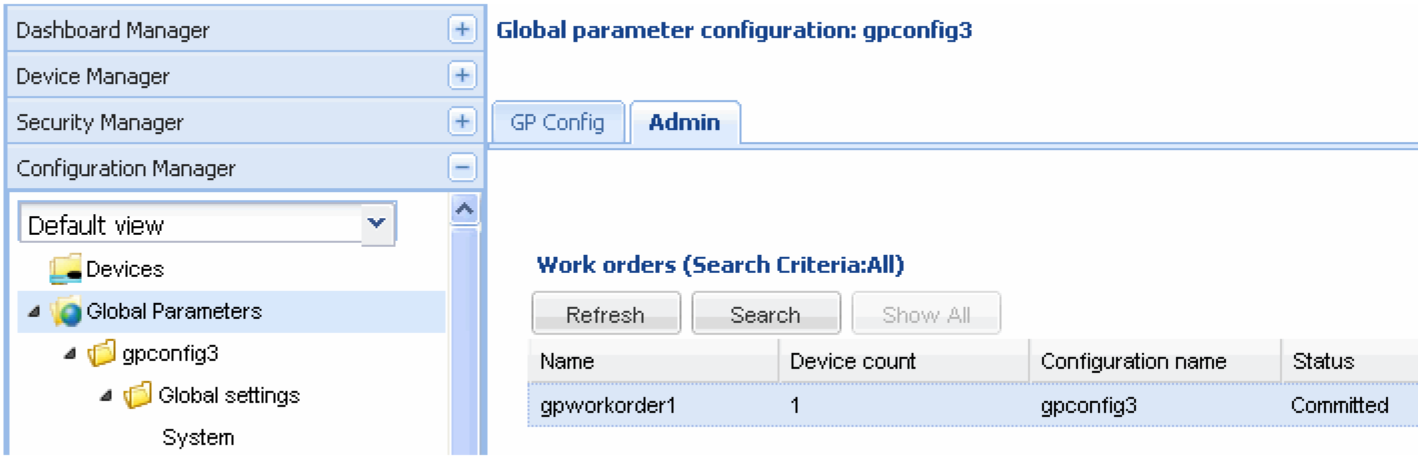
Global parameter configuration: gpconfig1

Local configuration view

Global configuration nam	Type	Name	Operation
gpconfig1	sip-config	sipConfig	created
gpconfig1	sip-manipulation	sipmanip1	created

Work Order Administration

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

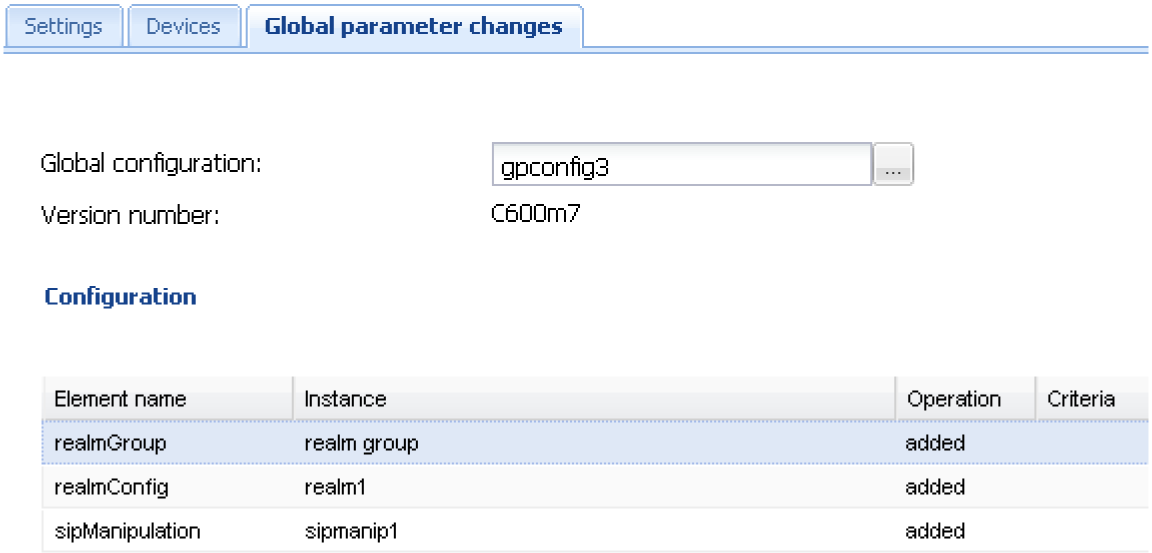


Global parameter configuration: gpconfig3

Work orders (Search Criteria:All)

Name	Device count	Configuration name	Status
gpworkorder1	1	gpconfig3	Committed

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.



Global configuration: gpconfig3

Version number: C600m7

Configuration

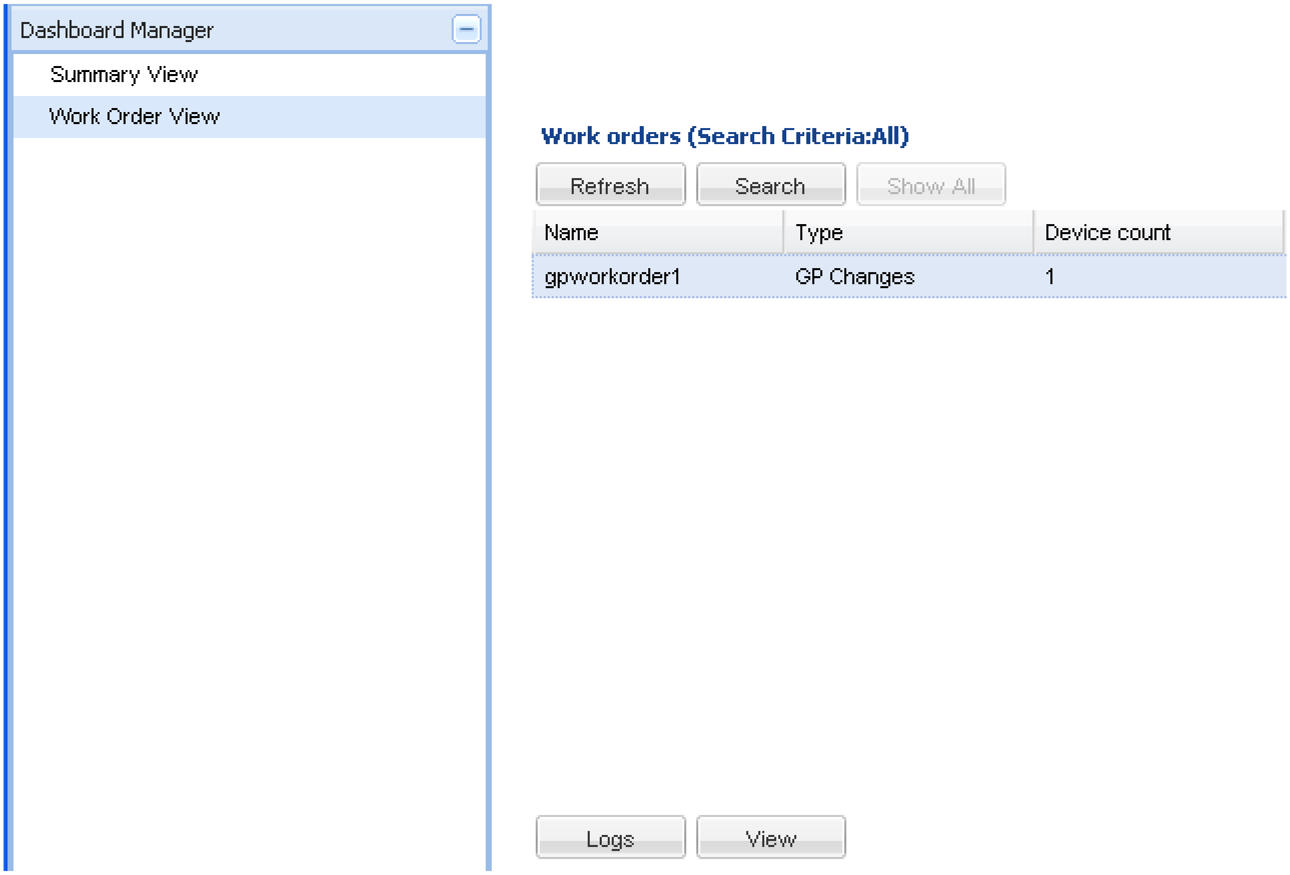
Element name	Instance	Operation	Criteria
realmGroup	realm group	added	
realmConfig	realm1	added	
sipManipulation	sipmanip1	added	

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.



Name	Type	Device count
gpworkorder1	GP Changes	1

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 Net-Net 4000 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 Delivery 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:

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:

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 Delivery 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 Delivery 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 Delivery 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:

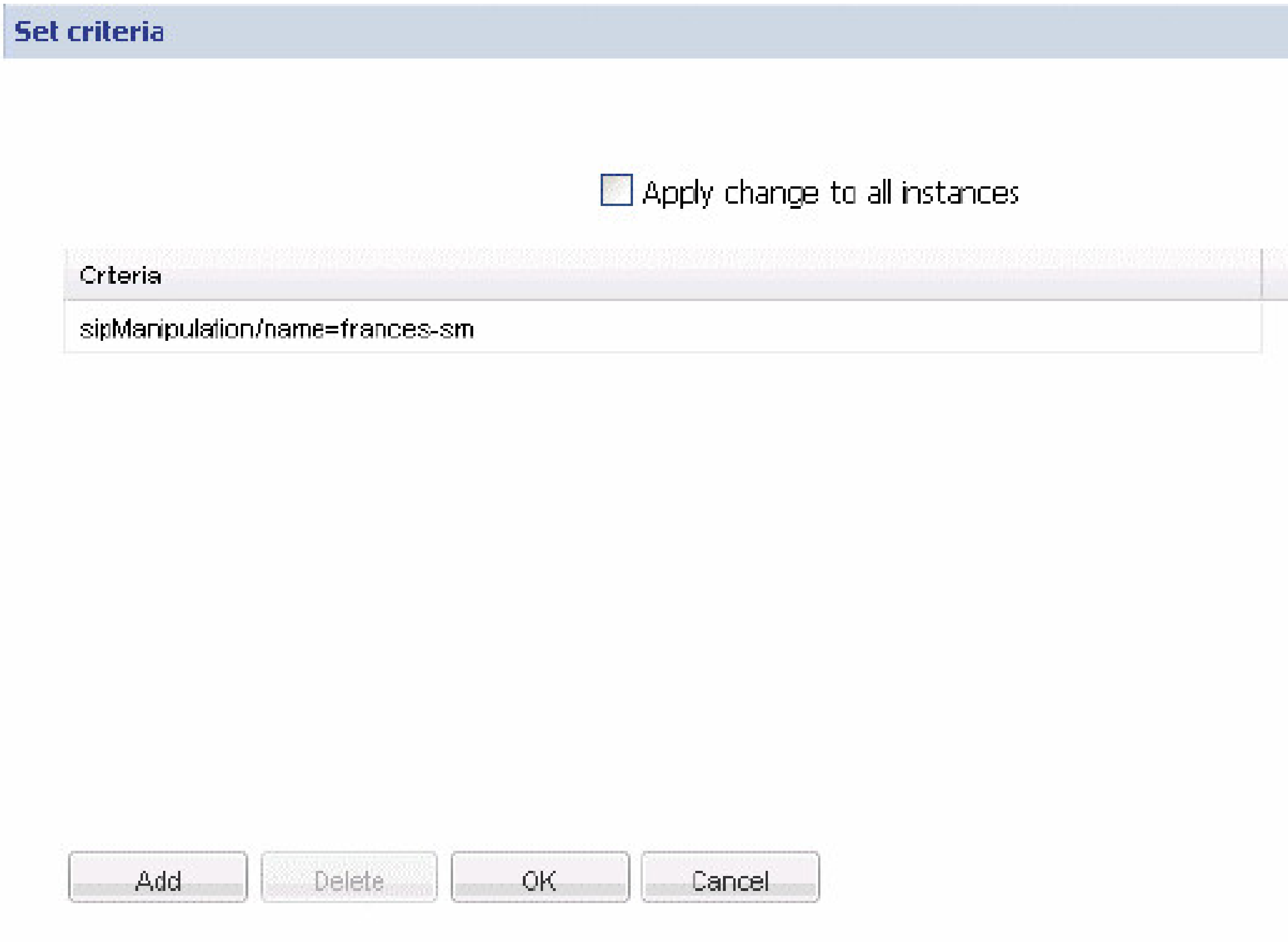
- Exactly match the specified instance. The instance is specified by using whatever “key” attribute values are appropriate for that type of configuration element. For example, in the case of a session agent the key is hostname.
- The system prompts you for input strings for each criteria.

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

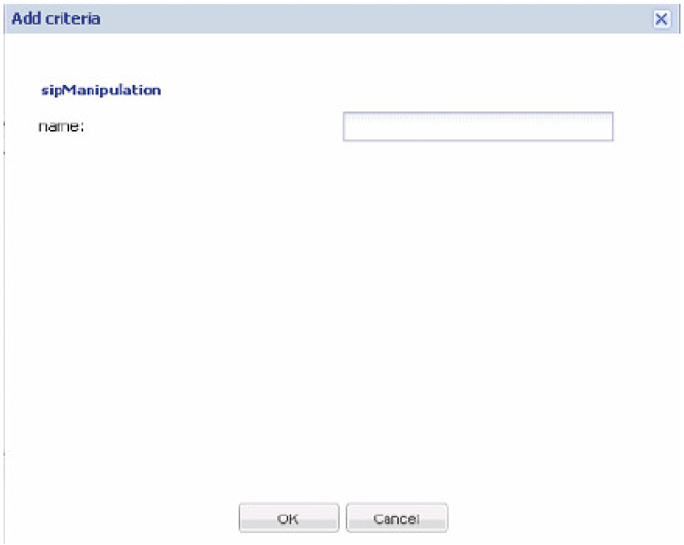
To set the criteria for an element in the work flow configuration:

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.



sipManipulation/name=frances-sm

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:

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:

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:

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:

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.

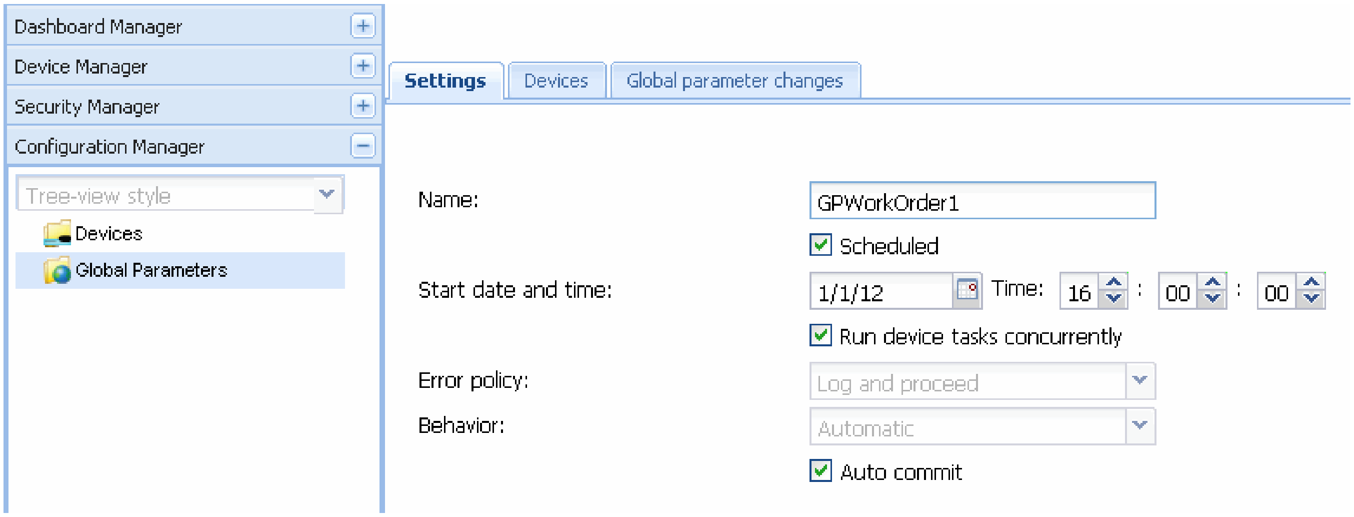
To enable auto commit:

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.



Name: GPWorkOrder1

☑ Scheduled

Start date and time: 1/1/12 Time: 16 : 00 : 00

☑ Run device tasks concurrently

Error policy: Log and proceed

Behavior: Automatic

☑ Auto commit

Adding Targeted Devices

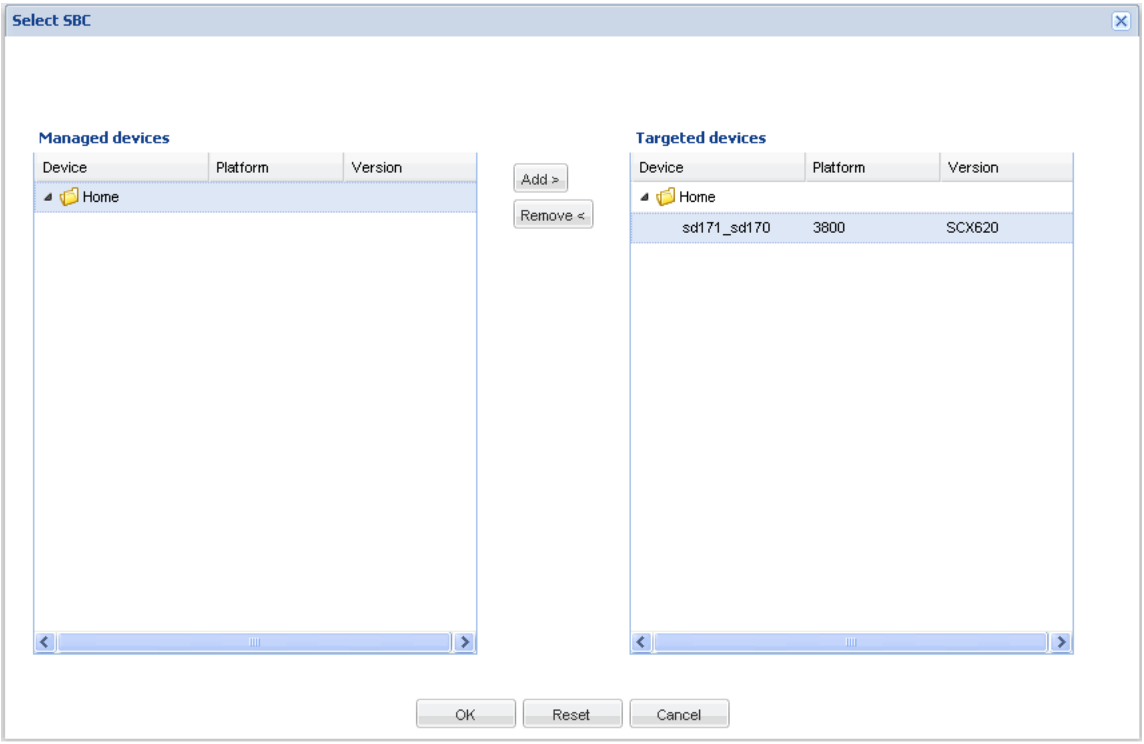
You add the targeted devices you want to apply to your work order.

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.



Managed devices

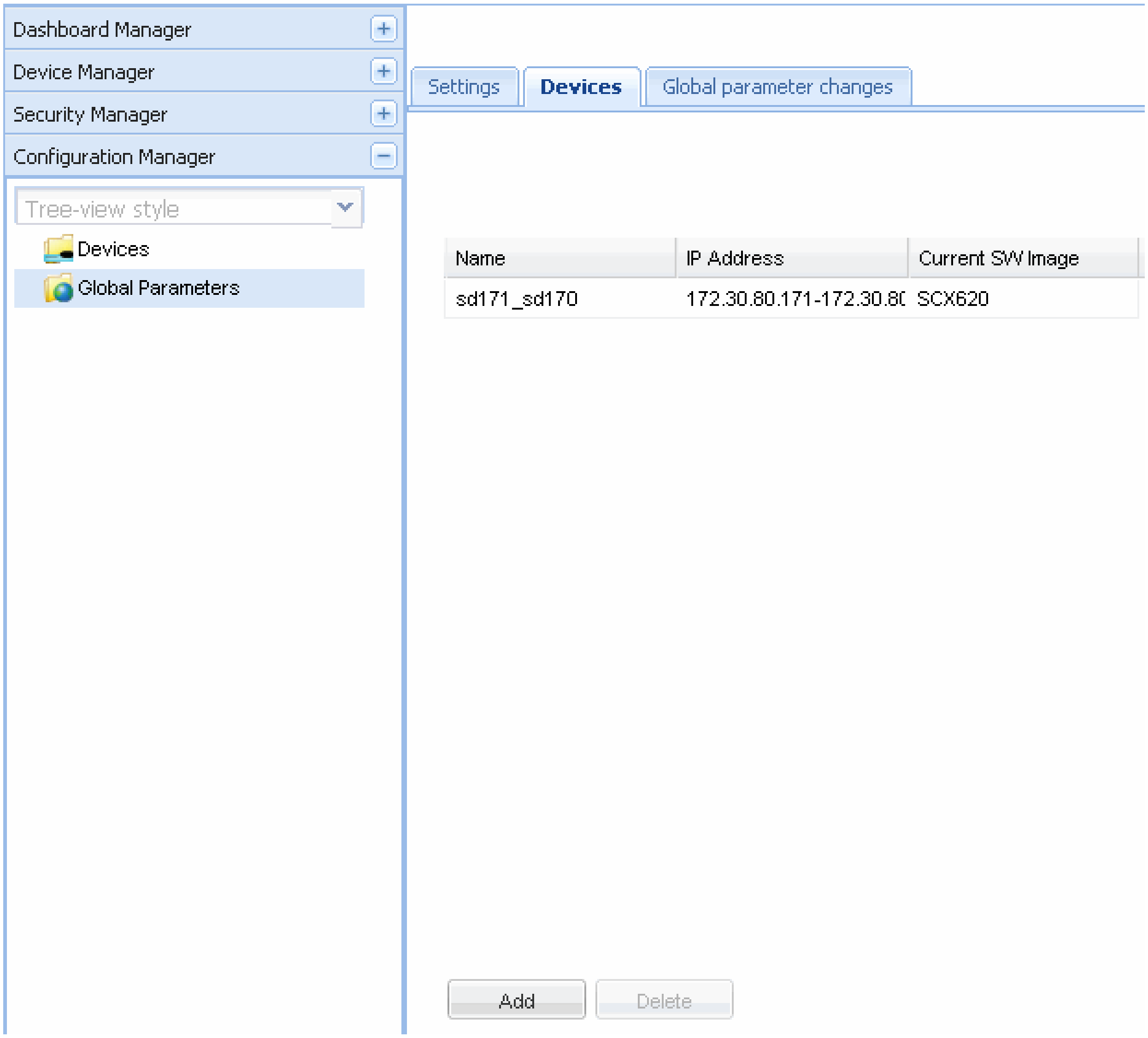
Device	Platform	Version
Home		

Targeted devices

Device	Platform	Version
Home		
sd171_sd170	3800	SCX620

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.



Name	IP Address	Current SW Image
sd171_sd170	172.30.80.171-172.30.8(	SCX620

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.

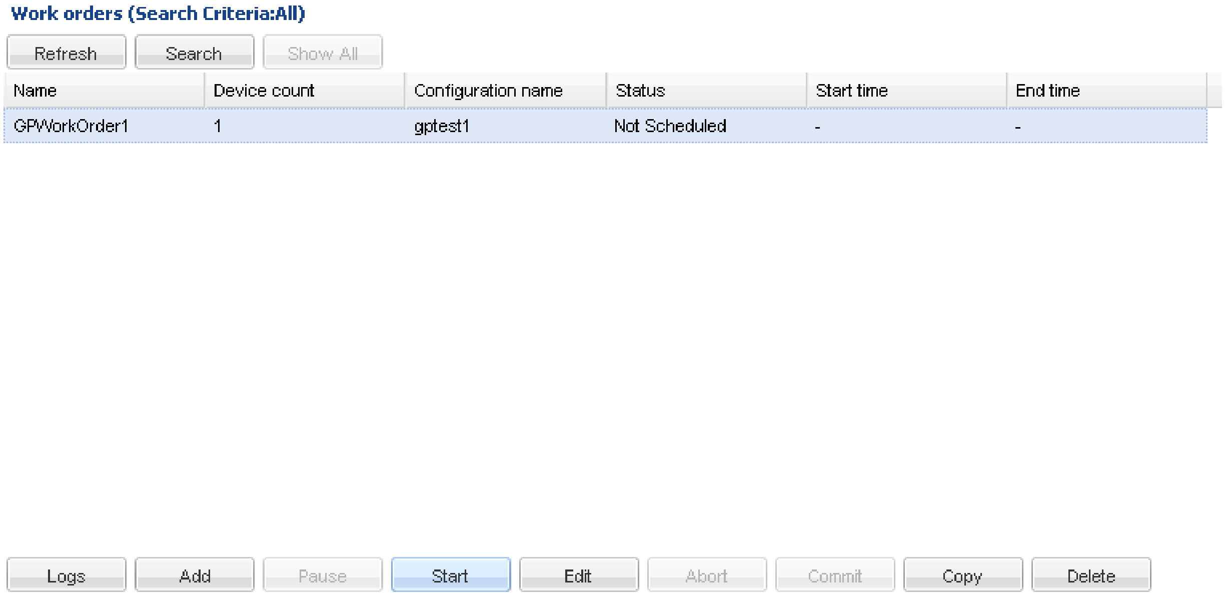
   If you set the time for a period that has passed, you will get an error message when you click Apply. Click OK to close the message, and click the Settings tab to correct the error.

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.



Work orders (Search Criteria:All)

Name	Device count	Configuration name	Status	Start time	End time
GPWorkOrder1	1	gptest1	Not Scheduled	-	-

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 Delivery 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.

Step	Description
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 Delivery 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 Delivery 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 Delivery 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 Delivery Manager server.

Work Order Processing States and User Actions Matrices

Depending on the Oracle Communications Session Delivery 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
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

States Below:	Action: Edit	Action: Delete	Action: Copy	Action: Commit	Action: Abort	Action: Start	Action: Restart	Action: Resume	Action: Pause
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 Delivery 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.

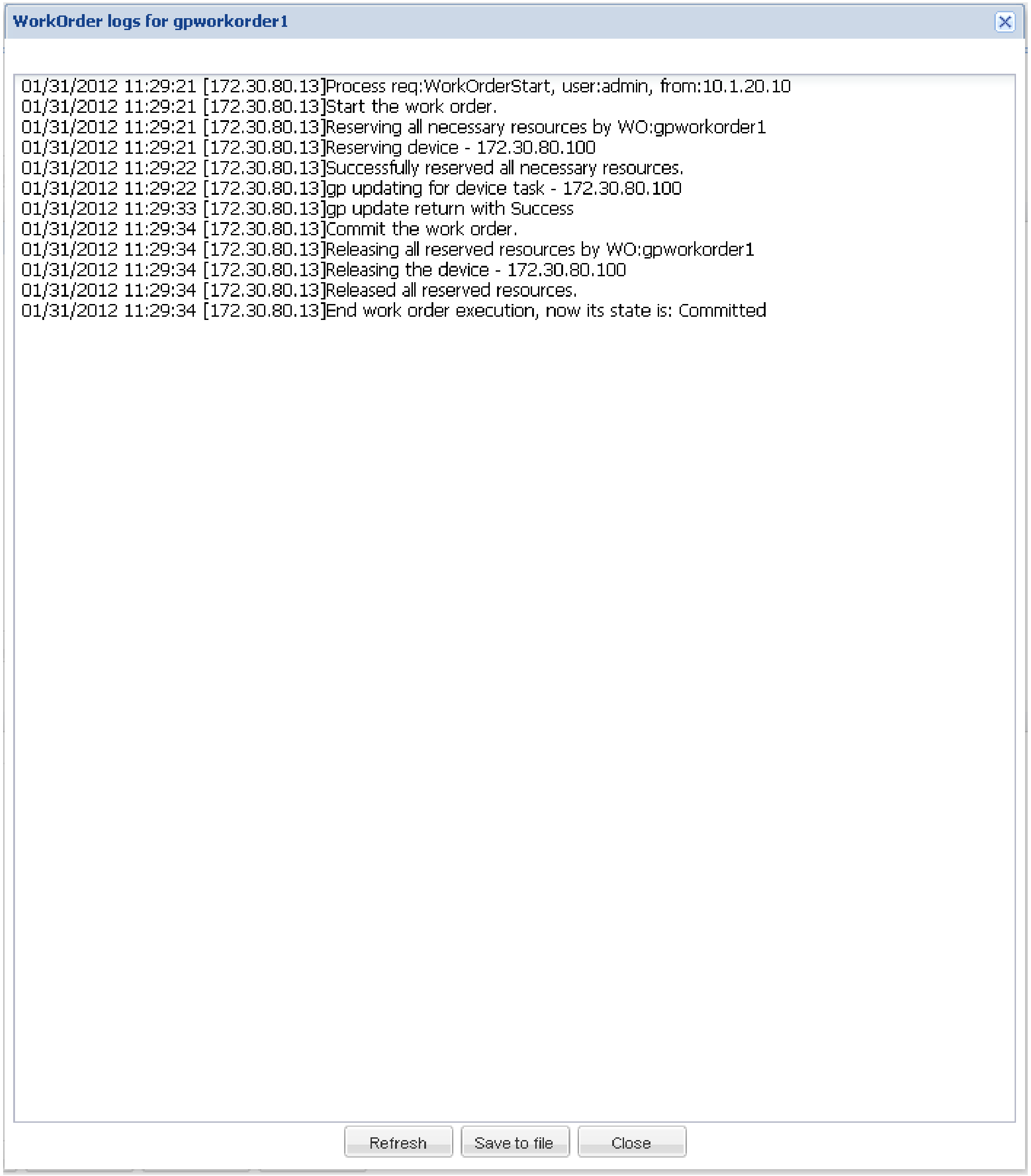
Logs

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

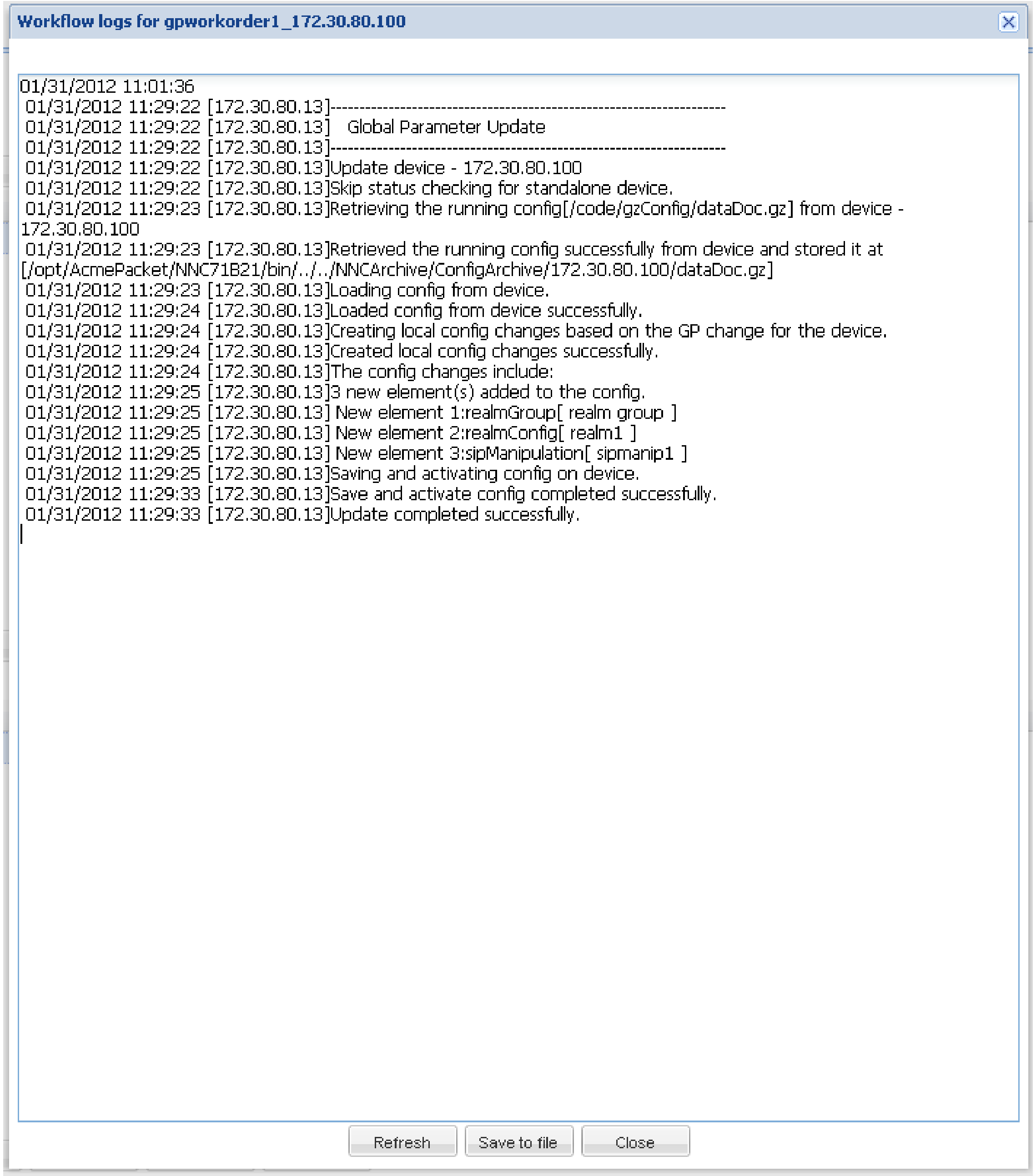
In the Work orders table, you can select a work order and click Logs. Work order-level messages pertain to the actions and state of the work order itself. You can view lower-level device tasks in the device tasks logs. Below is an example of a work order log.



```
01/31/2012 11:29:21 [172.30.80.13]Process req:WorkOrderStart, user:admin, from:10.1.20.10
01/31/2012 11:29:21 [172.30.80.13]Start the work order.
01/31/2012 11:29:21 [172.30.80.13]Reserving all necessary resources by WO:gpworkorder1
01/31/2012 11:29:21 [172.30.80.13]Reserving device - 172.30.80.100
01/31/2012 11:29:22 [172.30.80.13]Successfully reserved all necessary resources.
01/31/2012 11:29:22 [172.30.80.13]gp updating for device task - 172.30.80.100
01/31/2012 11:29:33 [172.30.80.13]gp update return with Success
01/31/2012 11:29:34 [172.30.80.13]Commit the work order.
01/31/2012 11:29:34 [172.30.80.13]Releasing all reserved resources by WO:gpworkorder1
01/31/2012 11:29:34 [172.30.80.13]Releasing the device - 172.30.80.100
01/31/2012 11:29:34 [172.30.80.13]Released all reserved resources.
01/31/2012 11:29:34 [172.30.80.13]End work order execution, now its state is: Committed
```

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.



```
01/31/2012 11:01:36
 01/31/2012 11:29:22 [172.30.80.13]----------------------------------------------------------------------
 01/31/2012 11:29:22 [172.30.80.13]   Global Parameter Update
 01/31/2012 11:29:22 [172.30.80.13]----------------------------------------------------------------------
 01/31/2012 11:29:22 [172.30.80.13]Update device - 172.30.80.100
 01/31/2012 11:29:22 [172.30.80.13]Skip status checking for standalone device.
 01/31/2012 11:29:23 [172.30.80.13]Retrieving the running config[/code/gzConfig/dataDoc.gz] from device -
172.30.80.100
 01/31/2012 11:29:23 [172.30.80.13]Retrieved the running config successfully from device and stored it at
[/opt/AcmePacket/NNC71B21/bin/../../NNCArchive/ConfigArchive/172.30.80.100/dataDoc.gz]
 01/31/2012 11:29:23 [172.30.80.13]Loading config from device.
 01/31/2012 11:29:24 [172.30.80.13]Loaded config from device successfully.
 01/31/2012 11:29:24 [172.30.80.13]Creating local config changes based on the GP change for the device.
 01/31/2012 11:29:24 [172.30.80.13]Created local config changes successfully.
 01/31/2012 11:29:24 [172.30.80.13]The config changes include:
 01/31/2012 11:29:25 [172.30.80.13]3 new element(s) added to the config.
 01/31/2012 11:29:25 [172.30.80.13] New element 1:realmGroup[ realm group ]
 01/31/2012 11:29:25 [172.30.80.13] New element 2:realmConfig[ realm1 ]
 01/31/2012 11:29:25 [172.30.80.13] New element 3:sipManipulation[ sipmanip1 ]
 01/31/2012 11:29:25 [172.30.80.13]Saving and activating config on device.
 01/31/2012 11:29:33 [172.30.80.13]Save and activate config completed successfully.
 01/31/2012 11:29:33 [172.30.80.13]Update completed successfully.
```

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.