

# One Voice Operations Center

Version 7.6



## Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from <https://www.audiocodes.com/library/technical-documents>.

This document is subject to change without notice.

Date Published: August-08-2019

## WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

## Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at <https://www.audiocodes.com/services-support/maintenance-and-support>.

## Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at <https://online.audiocodes.com/documentation-feedback>.

## Stay in the Loop with AudioCodes



## Related Documentation

Document Name
Mediant 500 MSBR User's Manual
Mediant 500L MSBR User's Manual
Mediant 500L Gateway and E-SBC User's Manual
Mediant 800B Gateway and E-SBC User's Manual
Mediant 800B MSBR User's Manual

Document Name
Mediant 1000B Gateway and E-SBC User's Manual
Mediant 1000B MSBR User's Manual
Mediant 2600 SBC User's Manual
Mediant 3000 User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
One Voice Operations Center Server Installation, Operation and Maintenance Manual
One Voice Operations Center Product Description
One Voice Operations Center Integration with Northbound Interfaces Guide
Device Manager Pro Administrator's Manual
Device Manager Express Administrator's Manual
ARM User's Manual
One Voice Operations Center Security Guidelines
One Voice Operations Center Alarms Guide

## Document Revision Record

LTRT	Description
91036	Initial document release for Version 7.4.
91037	Version 7.4 GA
91039	Updated to patch Version 7.4.1000. Network Map page   SIP Call Flow   QoE Link - regular expression   ARM SSO   RADIUS/LDAP SSO   Calls List – new columns   'Location' field   Show Grid   New AudioCodes logo and login screen   Hover cursor
91040	Calls List – 3-hour call. Timer defaults (0). Session Inactivity Period. Adding an Unprivileged User to MSSQL Server.
91041	Call Details page's PL parameter > 100%. Limitation note: Calls on HA devices unsupported. Backed-up filename format explanation.
91043	Connect to Ext. Apps: ARM. Endpoints License Allocation. Use Internal Mail Server (Alarms Forwarding) . FQDN (Add Device). 'IP Group Value' (Add Link)

LTRT	Description
91044	<p>Max number of alarms to aggregate in single email. Email alarms aggregation time interval. Connecting directly to the ARM. UMP. Sites. Device definition-generic option. NAT. Mandatory parameters indicated by *. SBC QoE – identify call by leg ID. SEM: Improved call identification, new call scenarios supported. AD users authentication with SfB SQL server. New authentication mode. Slider in QoE Thresholds and Status &amp; Alarm Settings. Call Flow in Call Details: message (arrow) selection sign. Alarm forward via mail - aggregate x alarms into a single mail. Topology Map: when icon location is changed, 'Save' button is enabled and highlighted orange. Fixed License Pool actions: Lock / Unlock, Reset Redundant, Switchover and Show. System &gt; Administration: Server Status and Info: new read-only screen. System &gt; License &gt; Summary: New 'Load License File' button.</p>
91045	<p>Dashboard. Load License. PM. External Applications. Max Concurrent Calls. Save Fixed LP Data to CSV. Force Operator Logout. Securing Connections with FQDN or IP Address. Custom Time Filter. Adding AC Device Manually. More Filters. Alarm Names. Backing Up. Restoring the Last Backup. Show Link. Adding an Active Directory. 'LDAP Connectivity DN'. Adding a cli File. Calls List - Save calls. SmartTAP. Floating License Server Address parameter (replaced DNS).</p>
91046	<p>User Defined Failure PM table</p>
91047	<p>ITSP Customer Multi-Tenant Architecture. 'Tenant Monitor Links User Group Name' field. Forwarding Alarms whose Destination Type is 'Notification'. Phones reflected in Journal page. Customizing Call Storage. Customizing max storage period. Notifications display time (sec). Test SBC. MSRP. Voice AI Gateway Service. Lync&gt;Skype. Floating License parameters. Hide Link Labels. Revert Local Changes. Search per IP/SN. Save Local Changes to Server. Combined Authentication Mode.</p>

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
	About the One Voice Operations Center	1
	Benefits	2
	Intended Audience	2
	Network Architecture	2
	ITSP Multi-Tenancy Architecture	3
	Enterprise Multi-Tenancy Architecture	3
	Non Multi-Tenancy Architecture	3
	Elements in Multi-Tenancy Architecture	4
	ITSP Customer Multi-Tenant Architecture	5
<b>2</b>	<b>Getting Started</b>	<b>6</b>
	Logging in	6
	Getting Acquainted with the Dashboard	6
	Getting Acquainted with the Network Topology Page	10
	Hovering Over a Cluster to Display Information	21
	Hovering Over a Device to Display Information	22
	Hovering over a Link to Display Information	23
	Returning to 'Home' Page by Clicking the AudioCodes Logo	23
	Getting Acquainted with the Network Map Page	23
	Configuring Operator Authentication	27
	Configuring Operator Authentication Centrally using an LDAP Server	28
	Configuring Operator Authentication Centrally with a RADIUS Server	31
	Viewing Operator Authentication in the Application Information Window	32
	Testing Connectivity with the LDAP / RADIUS Server	33
	Configuring Operator Authentication Locally, in the OVOC	34
	Adding an Operator	36
	How Multi Tenancy Impacts Operator Capabilities	36
	Adding a 'System' Operator	37
	Editing a 'System' Operator	42
	Deleting a 'System' Operator	42
	Deleting Multiple Operators	42
	Suspending a 'System' Operator	42
	Releasing a Suspended 'System' Operator	42
	Forcing a Password Change	42
	Forcing an Operator Logout	43
	Adding a 'Tenant' Operator	43
	Editing a 'Tenant' Operator	47
	Deleting a 'Tenant' Operator	47
	Deleting Multiple Operators	48
	Suspending a 'Tenant' Operator	48
	Releasing a Suspended 'Tenant' Operator	48
	Forcing a Password Change	48
	Forcing an Operator Logout	48

<b>3</b>	<b>Configuring Global (System) Settings</b>	<b>50</b>
	Administration tab	51
	Loading the OVOC Server License	51
	Making Sure your License Provides the Capabilities you Ordered	52
	Allocating Licenses to Tenants	53
	Authenticating Operators	56
	Determining OVOC Server Status	56
	Securing Connections with FQDN or IP Address	57
	Customizing Call Storage	58
	Customizing Maximum Storage Period	62
	Configuration tab	63
	Configuring Templates	63
	SNMP Connectivity	63
	HTTP Connectivity	65
	QoE Thresholds	65
	QoE Status and Alarms	67
	Configuring Alarms Settings	69
	Adding Configuration Files to the OVOC's Software Manager	72
	Adding the ini File	73
	Adding a cmp File	74
	Adding a cli File	75
	Adding Auxiliary Files	75
	Connecting Directly to External Applications	76
	Device Manager	77
	Reports	77
	ARM	78
	MasterScope	79
	Enabling Automatic Device Backup Periodically	80
	Tasks tab	81
	Displaying the Status of Tasks Currently Under Execution	82
<b>4</b>	<b>Defining your Network Topology</b>	<b>85</b>
	Adding a Tenant	85
	Adding a Region	91
	Adding AudioCodes Devices	92
	Adding AudioCodes Devices Automatically	92
	Adding AudioCodes Devices Manually	96
	Enabling Initial Connection Provisioning	102
	Before Enabling the Feature	104
	Enabling the Feature	104
	Making Sure First Time Provisioning was Successful	106
	Adding a Generic Device Manually	108
	Adding a Microsoft Skype for Business Device Manually	109
	Backing up a Device's Configuration using Backup Manager	112
	Manually Backing up a Device's Configuration	112
	Saving the Last Backed-up Configuration to your PC	113

Restoring the Last Backed-up Configuration to the Device .....	113
Adding Links .....	114
Adding Sites .....	118
Managing Endpoints .....	119
Dynamic Allocation of Endpoint Licenses .....	119
Configuring Endpoints .....	120
Monitoring Endpoints Status .....	121
Removing Endpoints from QoE Support .....	121
<b>5 Managing SBC Licenses .....</b>	<b>122</b>
Configuring SBC Floating License Monitoring .....	122
Configuring the OVOC for Floating License Monitoring .....	123
Adding an SBC to the Floating License .....	125
Performing Floating License Actions .....	128
Unmanage .....	129
Update .....	129
Reset .....	129
Register .....	129
Configuring OVOC-Floating License Service Communications .....	129
Viewing Floating License Summaries .....	130
Device Floating License Utilization Pane .....	130
Viewing Floating License Info .....	132
Viewing Device Info .....	132
Saving a Usage Data Report to your PC .....	133
Managing Device Licenses in the Fixed License Pool .....	134
Performing License Pool Actions .....	136
Applying a License to a Device from the Pool .....	136
Saving Fixed License Pool Data to CSV File .....	136
Before Performing 'Manage Device' / 'Update Device' .....	138
License Pool Alarms .....	139
<b>6 Assessing Network Health .....</b>	<b>140</b>
Assessing Health from the Network Summary .....	140
Assessing Health from the Network Topology Page .....	144
Filtering to Access Specific Information .....	147
Filtering by 'Time Range' .....	148
Filtering by 'Topology' .....	150
Filtering by 'Status' .....	152
Filtering by 'More Filters' .....	154
Determining Network Health from Alarms .....	155
Configuring Alarm Settings .....	155
Monitoring Active Alarms to Determine Network Health .....	155
Performing Management Actions on Active Alarms .....	155
Filtering by 'Severity' .....	158
Filtering by 'Source Type' .....	160
Filtering by 'More Filters' .....	161
Filtering by 'Type' .....	162

Filtering by 'Alarm Names' .....	163
Viewing Journal Alarms to Determine Operator Responsibility .....	163
Filtering the Alarms Journal by 'More Filters' .....	164
Viewing History Alarms .....	165
Filtering by 'Type' .....	166
Filtering by 'Alarm Names' .....	167
Forwarding Alarms .....	167
Forwarding Alarms whose Destination Type is 'SNMP' .....	173
Forwarding Alarms whose Destination Type is 'Mail' .....	176
Forwarding Alarms whose Destination Type is 'Syslog' .....	179
Forwarding Alarms whose Destination Type is 'Notification' .....	181
Viewing the New Rules in the Alarms Forwarding Page .....	184
Assessing Network Health in the Statistics Pages .....	184
Viewing Statistics on Calls over Devices .....	184
Metrics Bar Charts .....	185
Statistics Summary .....	187
Viewing Statistics on Streams over Links .....	187
Viewing Statistics on Calls over Sites .....	188
Viewing Statistics on Calls over Endpoints .....	188
Monitoring Performance .....	188
Adding a PM Template .....	189
Adding a PM Profile .....	193
Starting and Stopping PM Polling .....	196
Viewing PM Data Resulting from Polling .....	197
<b>7 Managing your Network .....</b>	<b>206</b>
Performing Management Actions .....	206
Updating Firmware .....	207
Updating Firmware on Multiple Devices .....	209
Resetting a Device .....	209
Locking or Unlocking a Device .....	209
Populating Links .....	211
Moving a Device .....	211
Backing Up .....	212
Restoring the Last Backup .....	213
Setting Configuration Factory Defaults .....	215
Saving a Device's Configuration File to Flash Memory .....	215
Saving a Device's Configuration File to the PC .....	215
Resetting Redundant .....	216
Performing Switchover .....	217
Changing Profile .....	217
Showing Device Information .....	219
Showing Link Information .....	220
Showing User Information .....	221
Editing a Device .....	223
Deleting a Device .....	223
Resetting a Device .....	224

Refreshing a Device's Pool License .....	225
Monitoring Device-Level Backup and Performing Rollback .....	225
<b>8 Obtaining Quality Statistics on Calls .....</b>	<b>226</b>
Accessing the Calls List .....	226
Filtering by 'Quality' .....	228
Filtering by 'More Filters' .....	230
Showing Call Details .....	232
Details of a Call Made over an AudioCodes SBC .....	232
Media .....	233
Signaling .....	236
Trends .....	237
SIP Call Flow .....	238
Details of a Test Call Made over an SBC .....	240
Call Details Page – Debug File Button .....	242
Details of a Call Made over Microsoft Skype for Business .....	242
Media .....	245
Signaling .....	246
Details of a Call Made over an Endpoint Using SIP Publish .....	247
Media .....	250
Managing QoE Thresholds Profiles per Tenant .....	252
Understanding the 3 Sensitivity-Level Profiles .....	252
Understanding How Call Color is Determined .....	253
Link Profile as Determinant .....	253
MOS Metric as Determinant .....	253
Adding a QoE Thresholds Profile per Tenant .....	254
Editing a QoE Thresholds Profile per Tenant .....	257
Deleting a QoE Thresholds Profile per Tenant .....	257
Managing QoE Status and Alarms per Tenant .....	258
Adding a QoE Alarm Rule per Tenant .....	258
Editing a QoE Alarm Rule per Tenant .....	261
Deleting a QoE Alarm Rule .....	261
<b>9 Getting Information on Users Experience .....</b>	<b>262</b>
Adding an Active Directory to the OVOC .....	262
Editing an Active Directory .....	265
Deleting an Active Directory .....	266
Synchronizing an AD with the AD Server .....	266
Assessing Overall End Users Experience .....	266
Assessing a Specific End User's Experience .....	268
Managing End Users .....	269
Filtering the User Details Page .....	270
<b>10 Producing Reports .....</b>	<b>271</b>
Using Reports Features .....	272
Producing a Network Status Report .....	275
Producing Trend Reports .....	279

---

Producing Top Users Reports .....	280
Scheduling a Report .....	282
Viewing a Scheduler Generated Report .....	284
Saving the File of a Scheduler Generated Report .....	284
Deleting the File of a Scheduler Generated Report .....	284
Editing a Schedule .....	284
Deleting a Schedule .....	284
Manually Running or Pausing a Schedule .....	285
<b>11 AudioCodes IP Network Telephony Equipment .....</b>	<b>286</b>
<b>12 Adding an Unprivileged User to MSSQL Server .....</b>	<b>291</b>



OVOC features:

- Highly scalable to support thousands of devices
- Multi-tenancy support for hosted and managed environments
- Auto-provisioning and configuration for the entire AudioCodes portfolio
- Real-time call quality monitoring and root cause analysis
- Integration with AudioCodes Routing Manager (ARM) session routing solution
- Centralized reporting and knowledge distribution

## Benefits

Here are some of the benefits you'll get from the OVOC:

- Facilitates easy and secure transition to VoIP deployments including UC, hosted business services and contact centers
- Reduces OpEx and TCO using centralized tools to remotely operate VoIP network components
- Simplifies and allows for more efficient device operation, administration and fault management
- Provides an intuitive real-time network view, capturing entire network status in real time
- Reduces MTTR with integrative detection and correction tools
- Delivers powerful analytic reports for effective planning of future network expansion and optimization
- Streamlines network management and quality monitoring in a single application
- Improves system availability with accurate troubleshooting and root cause analysis
- Increases efficiency with centralized configuration and provisioning
- Offers intelligent insights into network trends and performance to assist in planning and design
- Supports Microsoft Skype for Business environments

## Intended Audience

This *User's Manual* targets three audiences:

- The ITSP administrator whose network features multi-tenancy architecture and whose OVOC application will provide telephony management services to multiple enterprise customers (tenants) in their network. See [Network Architecture](#) below for more information.
- The enterprise administrator whose network does not feature multi-tenancy architecture and whose OVOC application will enable management of the enterprise's distributed offices. See also [Network Architecture](#) below.



The enterprise administrator whose network does not feature multi-tenancy architecture can skip documentation related to multi-tenancy.

- The enterprise administrator whose network features multi-tenancy architecture and whose OVOC application will provide telephony management services to multiple regional branches (tenants) in their network. See [Network Architecture](#) below for more information.

## Network Architecture

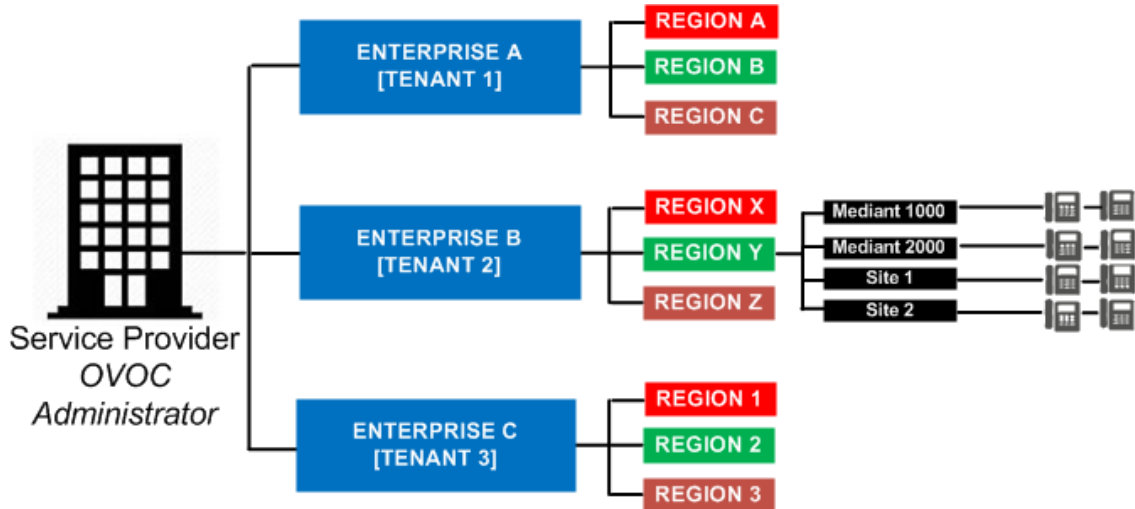
The OVOC features three types of telephony network architecture:

- Multi-Tenancy Architecture (see [ITSP Multi-Tenancy Architecture](#) on the next page and [Enterprise Multi-Tenancy Architecture](#) on the next page)
- Non Multi-Tenancy Architecture (see [Non Multi-Tenancy Architecture](#) on the next page)

## ITSP Multi-Tenancy Architecture

ITSP multi-tenancy architecture allows an Internet Telephony Service Provider (ITSP) administrator to deploy a single instance of the OVOC application to provide a telephony network management service to multiple enterprise customers (tenants).

**Figure 1-2: ITSP Multi-Tenancy Architecture**

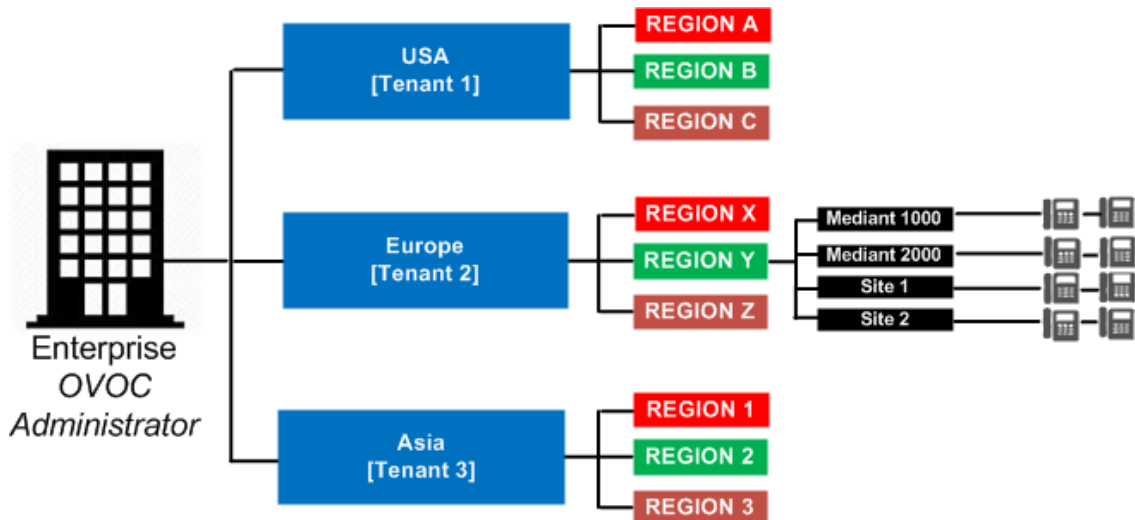


'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

## Enterprise Multi-Tenancy Architecture

Enterprise multi-tenancy architecture allows an enterprise administrator to deploy a single instance of the OVOC application in order to provide a telephony network management service to multiple regional branches (tenants).

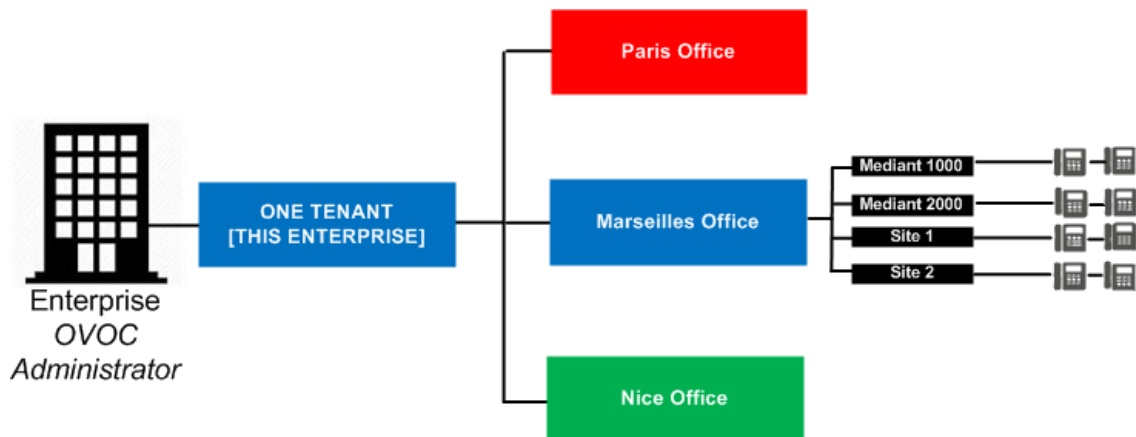
**Figure 1-3: Enterprise Multi-Tenancy Architecture**



'Tenants' can be given the capability to customize *parts* of the OVOC application, for example, the routing rules, but not to customize, for example, the OVOC server's roles.

## Non Multi-Tenancy Architecture

Non multi-tenancy architecture allows an enterprise's network administrator to define a single tenant (themselves) in order to provide a network management service to the enterprise's distributed offices.

**Figure 1-4: Non Multi-Tenancy Architecture - Enterprise**

## Elements in Multi-Tenancy Architecture

The following table shows OVOC application elements defined in multi-tenancy architecture.

**Table 1-1: OVOC Application Elements Defined in Multi-Tenancy Architecture**

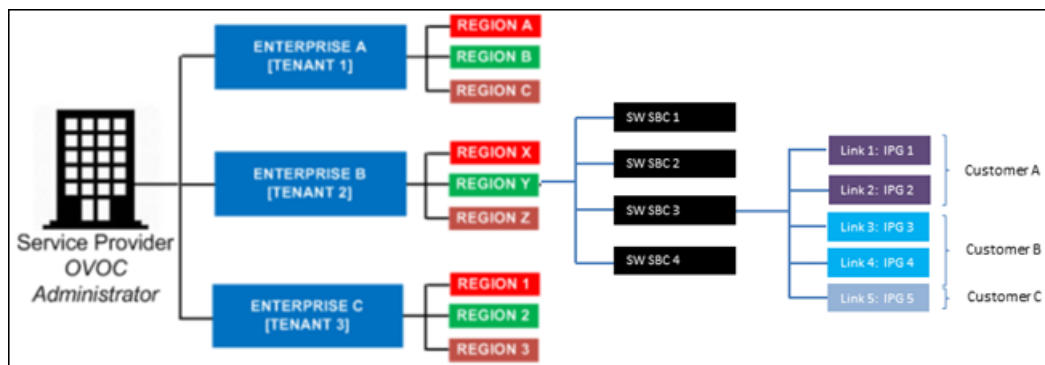
Element	Description
System	An ITSP managing multiple enterprises using a cloud-based or hosted 'global' OVOC application.
Tenant	<ul style="list-style-type: none"> <li>An ITSP's enterprise customer, using only a portion of the OVOC resources and only some of the OVOC entities. Other tenants (the ITSP's other enterprise customers) in the ITSP's multi-tenant network will be invisible to this tenant.</li> <li>An enterprise's regional branch, using only a portion of the OVOC resources and only some of the OVOC entities.</li> <li>An enterprise whose network administrator must define a tenant (that enterprise) under which to define the enterprise's distributed offices.</li> </ul>
Entity	Any element which can be managed or used as a whole: <ul style="list-style-type: none"> <li>Tenant entity (managed/assigned by a specific OVOC tenant)</li> <li>Global entity (managed by the OVOC system; applies to/affects all tenants)</li> <li>System entity (managed /assigned only by the OVOC system)</li> </ul>
Resource	Any element that can be partly managed/assigned: <ul style="list-style-type: none"> <li>Global resource (managed by the OVOC system; applies to/affects all tenants)</li> <li>Tenant resource (portion of the resource)</li> </ul>

## ITSP Customer Multi-Tenant Architecture

This architecture enables every OVOC operator (assigned to the same tenant), whose operator type is configured as 'Tenant' and whose operator security level is configured as 'Monitor Links', to monitor a *subset of links* under that tenant.

When an ITSP deploys this architecture, one operator can then monitor (for example) all links connecting customer 'A' to trunk groups while another operator can monitor (for example) all links connecting customer B's Microsoft Edge Server IP Group to its Skype for Business Front End IP Group.

**Figure 1-5: ITSP Customer Multi-Tenant Architecture**



The architecture features *non-bleeding partitions* between each subset of links so operators *cannot monitor the links of one another*.

OVOC operators in this architecture can monitor:

- Sites configured as links' destinations
- Devices configured as links' sources/destinations
- Links in the Network Topology page
- Link-related alarms and events
- Link-related statistics
- Link-related notifications for tasks and alarms

## 2 Getting Started

Getting started with the One Voice Operations Center involves logging in and getting acquainted with the management interface.



- Before getting started, make sure you have a correct OVOC license.
- For detailed information about the OVOC Server License, see [Loading the OVOC Server License](#) on page 51.

### Logging in

Logging in to the OVOC is a prerequisite to using the interface for network management.

➤ **To log in to the OVOC:**

1. Point your browser to the OVOC server's IP address: **https://<IP Address>**. You only need to enter its IP address; the rest of the URL is automatically added. Logging in can optionally be performed using FQDN rather than IP address.

**Figure 2-1: Login**

2. Enter your Username and Password:
  - **acladmin** (default) (case-sensitive) (can be modified later after defining users)
  - **pass\_1234** (default) (case-sensitive) (can be modified later after defining users)
3. The GUI by default displays the Dashboard.



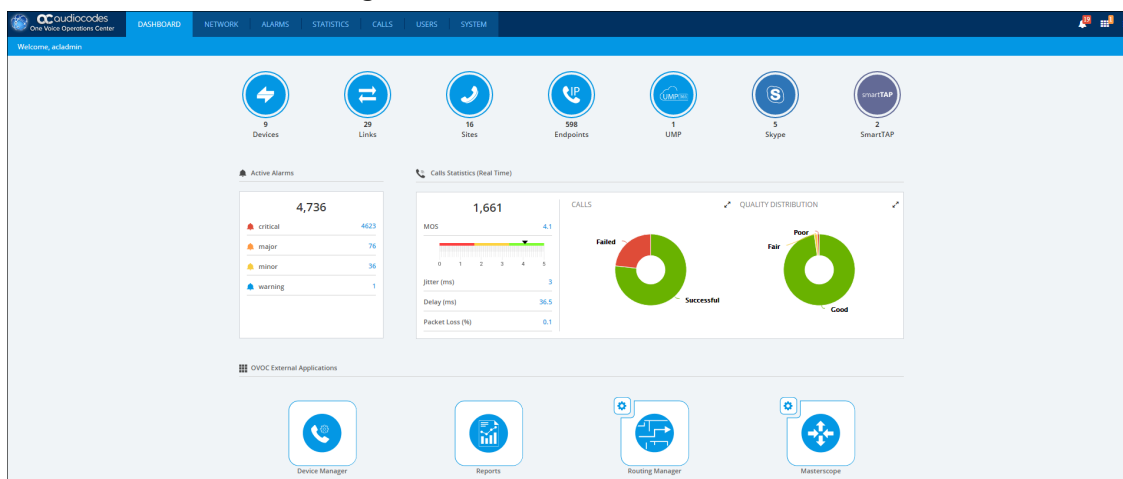
It's recommended to change the password after initial login.

### Getting Acquainted with the Dashboard

The Dashboard opens by default after logging in to the OVOC. The Dashboard gives the operator:

- an uncluttered, operator-friendly summary of the entire IP telephony network
- an aggregation of all IP telephony network information on a single page
- quick access to every entity, status, QoE and alarm from one central point


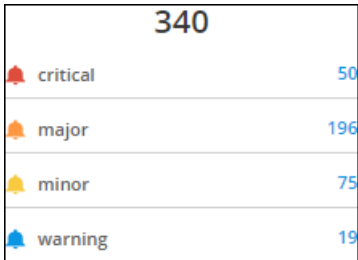

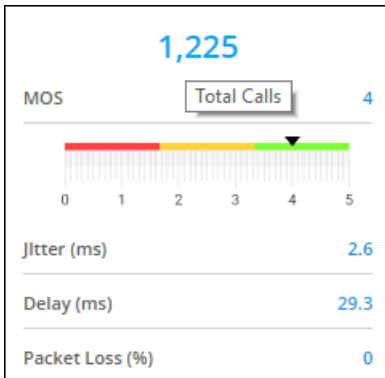

It may be helpful to get familiar with the page before getting started.







**Figure 2-2: Dashboard**

Use the following table as reference:

**Table 2-1: OVOC Dashboard**

Cluster Icon	Description
	[Devices] Indicates the number of AudioCodes SBC / MSBR / Gateway devices currently managed by the OVOC. Quickly accesses the Device Manage page filtered to display only these devices and none other.
	[Links] Indicates the number of links currently managed by the OVOC. Click to access the Links page. See <a href="#">Adding Links</a> on page 114.
	[Sites] Indicates the number of sites currently managed by the OVOC. Click to open the Sites page. See <a href="#">Adding Sites</a> on page 118
	[Endpoints] Indicates the number of endpoints currently managed by the OVOC. Click to open the Endpoints page. See <a href="#">Monitoring Endpoints Status</a> on page 121.
	[UMP] Indicates the number of User Management Packs (UMPs) 365 currently managed by the OVOC. For more information about the AudioCodes UMP 365, see under <a href="#">AudioCodes IP Network Telephony Equipment</a> on page 286.
	[Skype] Indicates the number of Microsoft Skype for Business entities, for example, Front End Servers, currently managed by the OVOC. Click to access the Device Management page.
	[SmartTAP] Quickly accesses the OVOC's Device Management page filtered to display only the SmartTAP Application server. The AudioCodes SmartTap for Microsoft Skype for Business is an intelligent, fully certified and secured enterprise interactions recording solution of voice, video and IMs. With SmartTAP, enterprises can capture and index any customer or organizational interaction across external and internal communication channels seamlessly. Note that for OVOC-SmartTAP server connectivity, Microsoft's SNMP Service must be disabled on the SmartTAP server.

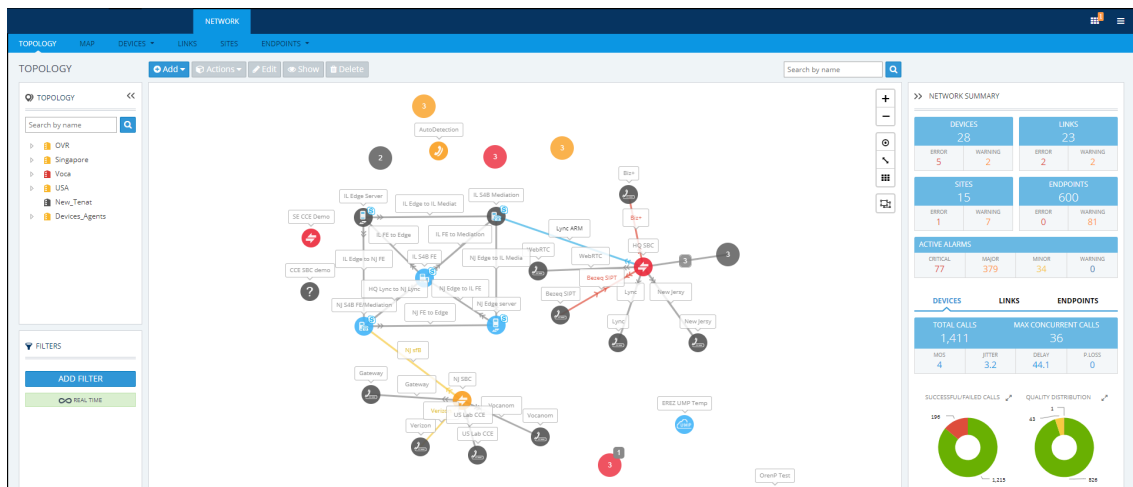
Cluster Icon	Description
 Active Alarms	<p>Indicates (1) the total number of active alarms in the network and (2) the number of active Critical, Major, Minor and Warning severity-level alarms.</p>  <ul style="list-style-type: none"> <li>■ Clicking the total number of active alarms in the network opens the Active Alarms page.</li> <li>■ Clicking the row of a severity level opens the Active Alarms page filtered by that severity level, so operators can directly access only alarms whose severity level is (for example) critical; the Alarms page opens displaying only critical severity-level alarms. In the Alarms page, operators can select any critical severity-level alarm to view its details.</li> </ul>
 Calls Statistics	<ul style="list-style-type: none"> <li>■ Indicates (1) the total number of calls, in real time and (2) the average MOS, Jitter, Delay and Packet Loss (%) scores:</li> </ul>  <ul style="list-style-type: none"> <li>✓ With a click, the operator can directly access the Statistics page displaying statistics on all calls (Total Calls).</li> <li>■ Indicates below left (1) Successful / Failed Calls and below right (2) Quality Distribution (Good, Fair, Poor):</li> </ul>  <ul style="list-style-type: none"> <li>✓ [Refer to above left] With a click, the operator can directly access only calls whose performance status is FAILED (for example); the Calls List page opens displaying only failed calls. In the Calls List page, the operator can select any call and show its details in the Call Details page that opens.</li> </ul>

Cluster Icon	Description
	<p>✓ [Refer to above right] With a click, the operator can directly access only calls whose quality is assessed to be Poor (for example); the Calls List page opens displaying only poor quality calls. In the Calls List page, the operator can select any call and show its details in the Details dynamic tab that opens.</p>
 External Applications	<p>Each external application described next opens in a separate browser tab or browser window depending on the operator's browser settings.</p>
	<p>[Device Manager] Quickly accesses the Device Manager, the AudioCodes life cycle management application for enterprise IP telephony deployments that enables administrators to deliver a reliable desktop phone service within their organization. With the ability to deploy and monitor IP telephony devices, identify problems, and then fix them rapidly and efficiently, the application enhances employee satisfaction, increases productivity and lowers IT expenses.</p>
	<p>[Reports] Quickly accesses reports-generation capability that operators can utilize to distribute session experience data and comparative analysis to responsible persons within the enterprise and to external authorities associated with the enterprise's IP telephony network, for accurate diagnosis and correction of degraded sessions and for general network optimization.</p>
	<p>[Routing Manager] Quickly accesses the Routing Manager (ARM) for managing the dial plan and call routing rules of multi-site, multi-vendor enterprise VoIP networks. The ARM enables centralized control of all session routing decisions. Through ARM's graphical user interface, network administrators can design and modify their voice network topologies and call routing policies from a single location, resulting in significant time and cost savings. Time-consuming tasks such as adding a new PSTN or SIP trunk interconnection, adding a new branch office or modifying individual users' calling privileges can be carried out simply and rapidly.</p> <p>Note that the icon is never disabled even when the ARM is disconnected; if the ARM is disconnected, the AudioCodes website page related to the ARM opens instead.</p>
	<p>[MasterScope] Applies only to operators who have acquired and installed NEC's MasterScope. Enables connecting directly to MasterScope in order to quickly and easily access the exact network equipment component associated with a voice quality issue - if an issue is detected - and benefit from root cause analysis.</p>
<p>Notifications</p> 	<p>Notifications can be configured to pop up in the uppermost right corner when a task is performed or when an alarm is received. The bell icon indicates the number of notifications that have not yet been viewed; the color indicates highest alarm severity level. Clicking the bell opens the notifications list. In the list, operators can delete a notification, delete all notifications or click a notification to open the Tasks page or Alarms History page. The display time can be changed. The feature can be switched off.</p>

## Getting Acquainted with the Network Topology Page

It may be helpful to briefly familiarize yourself with the OVOC's central page - the Network Topology page - before getting started.

**Figure 2-3: OVOC GUI – Network Page – Topology**



The page is divided into three panes: left, middle and right.

In the left pane, the 'tree' displays network entities, up to the level of tenant (first-level navigation).







The middle pane displays a topological view of devices and links in the network on which operators can quickly obtain basic device information and statuses and perform actions (second-level navigation).






The right pane displays a summary of network statistics from which operators can determine network health.












Each entity can be viewed in table view. The following table explains the entity icons in the Network Topology page. Icon colors are propagated from the statuses of the entities. Entity status is derived from management status, voice quality status and license status.




**Table 2-2: Network Topology – Network Entities and Statuses**


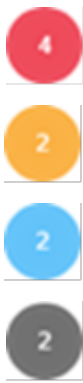
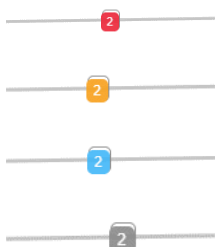
Network Entity	Icon	Explanation
Tenant		<p>For detailed information about multi-tenancy architecture, see <a href="#">ITSP Multi-Tenancy Architecture</a> on page 3.</p> <p> = Tenant status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of at least one region is Error</li> <li>✓ voice quality status of at least one region is Error</li> <li>✓ license status of at least one region is Error</li> <li>✓ license status of the tenant itself is Error due to one of these [Critical] alarms: QoE Devices Overload, QoE Sessions Overload, QoE Endpoints Overload or Endpoints Management Overload.</li> </ul> <p> = Tenant status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of at least one region is Warning</li> </ul>



Network Entity	Icon	Explanation
		<ul style="list-style-type: none"> <li>✓ voice quality status of at least one region is Warning</li> <li>✓ license status of at least one region is Warning</li> <li>✓ license status of the tenant itself is Warning due to one of these [Major] alarms: QoE Devices Overload, QoE Sessions Overload, QoE Endpoints Overload or Endpoints Management Overload.</li> <li>✓ One of the tenant's AD is disconnected</li> </ul> <p> = Tenant status is OK when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of all regions is OK or Unmonitored</li> <li>✓ voice quality status of all regions is OK or Unmonitored</li> <li>✓ license status of all regions is OK or Unmonitored</li> <li>✓ license status of the tenant itself is free of alarms</li> <li>✓ All the tenant's ADs are connected</li> </ul> <p> = Tenant status is Unmonitored when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of all regions is Unmonitored</li> <li>✓ voice quality status of all regions is Unmonitored</li> <li>✓ license status of all regions is Unmonitored</li> </ul>
Region		<p> = Region status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of at least one device or site is Error</li> <li>✓ voice quality status of at least one device or site is Error</li> <li>✓ license status of at least one device or site is Error</li> </ul> <p> = Region status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of at least one device or site is Warning</li> <li>✓ voice quality status of at least one device or site is Warning</li> <li>✓ license status of at least one device or site is Warning</li> </ul> <p> = Region status is OK when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of all devices and sites is OK or Unmonitored</li> <li>✓ voice quality status of all devices and sites is OK or Unmonitored</li> <li>✓ license status of all devices and sites is OK or Unmonitored</li> </ul>

Network Entity	Icon	Explanation
		<p> = Region status is Unmonitored when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of all devices and sites is Unmonitored</li> <li>✓ voice quality status of all devices and sites is Unmonitored</li> <li>✓ license status of all devices and sites is Unmonitored</li> </ul>
Device	  	<p>Indicates an SBC belonging to AudioCodes communicating with the OVOC.</p> <p>Red = Device status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is Error (if device alarms status or connection status is disconnected)</li> <li>✓ voice quality status is Error (if control status or media status is Error, or if connection status is disconnected)</li> <li>✓ License status is Error only if license pool is failed or expired</li> </ul> <p>Orange = Device status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is Warning (if device alarms status or administration status is Warning)</li> <li>✓ voice quality status is Warning (if control status or media status or connection status is Warning)</li> <li>✓ license status is Warning (if a reset/apply action is required in the license pool or if there is no management license in the device or if there is no voice quality license)</li> </ul> <p>Blue = Device status is OK when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is OK - Clear or Undetermined (if device alarms status or connection status is OK - Clear or Undetermined)</li> <li>✓ voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined)</li> <li>✓ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined)</li> </ul> <p>Strikethrough = locked No strikethrough = unlocked</p>
UMP		<p>Indicates the AudioCodes User Management Pack 365 communicating with the OVOC.</p> <p>Red = UMP status is Error when one or more of the following exists:</p>

Network Entity	Icon	Explanation
	 	<ul style="list-style-type: none"> <li>✓ management status is Error (if UMP alarms status or connection status is disconnected)</li> <li>✓ voice quality status is Error (if control status or media status is Error, or if connection status is disconnected)</li> <li>✓ License status is Error only if license pool is failed or expired</li> </ul> <p>Blue = UMP status is OK when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is OK - Clear or Undetermined (if UMP alarms status or connection status is OK - Clear or Undetermined)</li> <li>✓ voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined)</li> <li>✓ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined)</li> </ul> <p>Orange = UMP status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is Warning (if UMP alarms status or administration status is Warning)</li> <li>✓ voice quality status is Warning (if control status or media status or connection status is Warning)</li> <li>✓ license status is Warning (if a reset/apply action is required in the license pool or if there is no management license in the UMP or if there is no voice quality license)</li> </ul> <p>Strikethrough = locked No strikethrough = unlocked</p>
Microsoft Skype for Business Device	  	 = Microsoft Skype for Business Mediation Server  = Microsoft Skype for Business Edge Server  = Microsoft Skype for Business Front End Server
Generic Device		<p>Indicates a non-AudioCodes device or entity that is also part of the OVOC network topology: IP PBX (shown on left), SIP trunk, other vendors' SBC / gateway. These devices participate in processing OVOC network calls and are connected to devices.</p>
Site	 	<p>Color and status are propagated from the endpoints under the site.</p> <p>Gray = Site status is Unmonitored when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status of all endpoints is Unmonitored</li> <li>✓ voice quality status of all endpoints is Unmonitored</li> </ul>

Network Entity	Icon	Explanation
	 	<ul style="list-style-type: none"> <li>✓ license status of all endpoints is Unmonitored</li> </ul> <p>Blue = Site status is OK when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is OK - Clear or Undetermined (if site alarms status or connection status is OK - Clear or Undetermined)</li> <li>✓ voice quality status is OK - Clear or Undetermined (if control status or media status or connection status is OK - Clear or Undetermined)</li> <li>✓ license status is OK - Clear or Undetermined (if license pool status is OK - Clear or Undetermined)</li> </ul> <p>Orange = Site status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is Warning (if site alarms status or administration status is Warning)</li> <li>✓ voice quality status is Warning (if control status or media status or connection status is Warning)</li> <li>✓ license status is Warning (if a reset/apply action is required in the license pool or if there is no management license in the site or if there is no voice quality license)</li> </ul> <p>Red = Site status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ management status is Error (if site alarms status or connection status is disconnected)</li> <li>✓ voice quality status is Error (if control status or media status is Error, or if connection status is disconnected)</li> <li>✓ License status is Error only if license pool is failed or expired</li> </ul>
Link		<p>A link joins two devices:</p> <p>Red = Voice quality status is Error when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ 'Critical' Control Status</li> <li>✓ 'Critical' Media Status</li> </ul> <p>Orange = Voice quality status is Warning when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ 'Major' Control Status</li> <li>✓ 'Major' Media Status</li> </ul> <p>Blue = Voice quality status is OK/Clear when one or more of the following exists:</p> <ul style="list-style-type: none"> <li>✓ Control Status is OK/Clear</li> <li>✓ Media Status is OK/Clear</li> <li>✓ Control Status or Media Status is Unmonitored</li> </ul> <p>Gray = Voice quality status is Unmonitored when both of these exist:</p>

Network Entity	Icon	Explanation
		<ul style="list-style-type: none"> <li>✓ Control Status is Unmonitored</li> <li>✓ Media Status is Unmonitored</li> </ul> <p><b>Note:</b></p> <ul style="list-style-type: none"> <li>✓ If no voice quality license exists, status will be Unmonitored.</li> <li>✓ Link status does not impact device / region</li> <li>✓ Under the link's name tag, a single arrow indicates the link's direction: ingress (calls incoming to the reporting device) or egress (calls outgoing from the reporting device); if there are no arrows under the link's name tag, the link is bi-directional. In the figure below, the link is ingress, to NJ SBC.</li> <li>✓ A double arrow located next to one of the devices indicates that it is the reporting device. In the figure below, the reporting device is NJ SBC.</li> </ul> 
Device clusters		<p>Indicate aggregated clusters of devices (AudioCodes devices as well as non-AudioCodes devices). The numbers indicate how many devices are in the cluster.</p> <ul style="list-style-type: none"> <li>■ Red = at least one entity in this cluster has a status of Error – see above in this table for the one or more conditions that need to exist for status to be Error</li> <li>■ Orange = at least one entity in this cluster has a status of Warning – see above in this table for the one or more conditions that need to exist for status to be Warning</li> <li>■ Blue = at least one entity in this cluster has a status of OK – see above in this table for the one or more conditions that need to exist for status to be OK</li> <li>■ Gray = at least one entity in this cluster has a status of Unmonitored – see above in this table for the one or more conditions that need to exist for status to be Unmonitored</li> </ul>
Link clusters		<p>Square icons indicate aggregated clusters of links. The link indication can be on a line representing a link (left upper) or adjoined to a device cluster (left lower). The number in each square indicates how many links are in the cluster.</p> <ul style="list-style-type: none"> <li>■ Red square = at least one link in this cluster has a voice quality status of Error – see above in this table for the one or more conditions that need to exist for voice quality status to be Error</li> <li>■ Orange square = at least one link in this cluster has a voice quality status of Warning – see above in this table for the one or more conditions that need to exist for voice quality status to be Warning</li> </ul>

Network Entity	Icon	Explanation
		<ul style="list-style-type: none"> <li>■ Blue square = at least one link in this cluster has a status of OK – see above in this table for the one or more conditions that need to exist for status to be OK</li> <li>■ Gray square = at least one link in this cluster has a voice quality status of Unmonitored – see above in this table for the two conditions that need to exist for voice quality status to be Unmonitored</li> </ul>
SmartTAP		<p>Indicates the AudioCodes SmartTAP communicating with the OVOC.</p> <ul style="list-style-type: none"> <li>■ Red = SmartTAP status is Error when management status is Error (if SmartTAP alarms status or connection status is disconnected)</li> <li>■ Orange = SmartTAP status is Warning when management status is Warning (if SmartTAP alarms status or administration status is Warning)</li> <li>■ Blue = SmartTAP status is OK when management status is OK - Clear or Undetermined (if SmartTAP alarms status or connection status is OK - Clear or Undetermined)</li> <li>■ Gray = SmartTAP status is Unmonitored when management status is unmonitored</li> </ul>

The following bar of icons is displayed on the right side of the Network Topology page.



From top to bottom:

- Click **+** or **-** to zoom in or out of the map.
- Click the **Center Map** button to center the map in the page - useful if the previous operator dragged it off center.
- Click the **Save Local Changes to Server** button after making a change to the network topology, for example, after dragging a device to a different location. The button is only displayed *if a change is made*. It's highlighted orange. After saving the change, the button disappears.
- Click the **Revert Local Changes** button after making a change to the network topology, for example, after dragging a device to a different location. This button is only displayed *if a change is made*. It's highlighted orange. It allows you to revert to the network topology that existed before you made the change instead of saving the changed network topology. After reverting, the button disappears.
- Click the **Create Links** button to create a link.

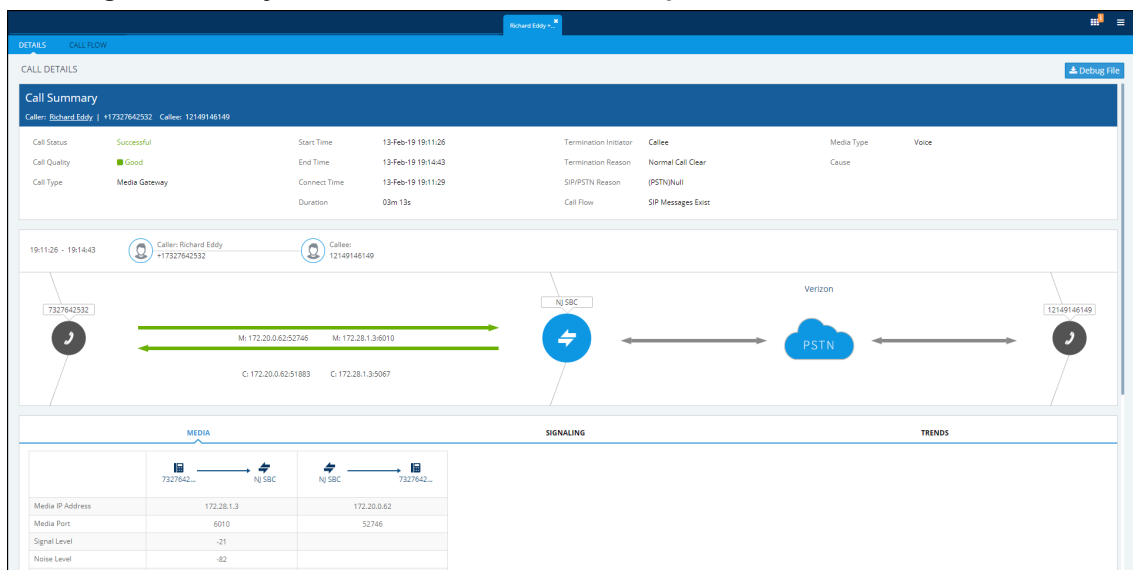
- The **Show Grid** button allows operators to display gridlines; the background of the Network Topology page is by default white.
- The **Hide Link Labels** button allows operators to hide the labels of the links in the Network Topology and Network map pages; this reduces clutter for more effective management, especially in networks with many devices and links.
- **Show Clusters.** If more than 200 devices and sites (aggregated) are defined, the button will not be available and the page will *automatically* be displayed in clusters. The button will only be available if fewer than 200 devices and sites (aggregated) are defined. The feature reduces clutter and improves operational efficiency.
  - When the clusters feature is activated, enter in the 'Search' field the name or a part of the name of an entity to locate; the circumferences of the clusters containing an entity with that name segment are colored purple. You can hover over each to determine from a pop-up which one contains the entity you're after. In clusters containing too many entities to scan through, you can use the pop-up's 'Search' feature to facilitate the search (see also under [Hovering Over a Cluster to Display Information](#) on page 21).

Select an area: Press the Shift key and press the mouse.

The Network Topology page lets you quickly drill down from a tenant to the core of an issue. Fast access to very specific information makes network management efficient. This capability earns OVOC the title of 'expert system'.

Specific information related to device, user and call is automatically dynamically tabbed on the menu bar, facilitating quick and easy future access and troubleshooting:

**Figure 2-4: Dynamic Tab for Fast Access to Specific Information**



For more information about the dynamic tab that is created for call details, see [Showing Call Details](#) on page 232.

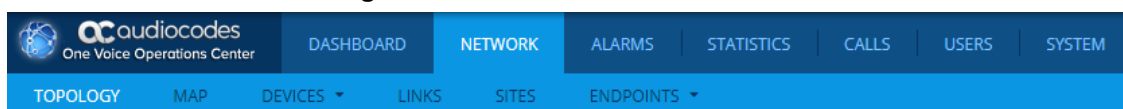
For more information about the dynamic tab that is created for user details, see [Assessing a Specific End User's Experience](#) on page 268.

A dynamic tab lets you quickly access a specific page that is automatically dynamically tabbed on the menu bar after for example drilling down in the Topology page from a tenant to the core of an issue. The tab allows quick and easy future access to specific information related to device, user, call, etc., displayed in the page. It can be deleted from the menu bar at any time. The feature simplifies troubleshooting management.

The right pane of the Network Topology page summarizes device statuses and alarms in the network.

The following figure shows the OVOC's menu bar.

**Figure 2-5: Menu Bar**



Use the following table as reference to the preceding figure. See also [Getting Acquainted with the Dashboard](#) on page 6.

**Table 2-3: Menu Bar**

Menu	Tab	Description
Network	Topology	<p>The tab's page lets you:</p> <ul style="list-style-type: none"> <li>■ Assess at a glance the topology of the network</li> <li>■ Perform multiple configuration and maintenance actions</li> <li>■ Select multiple devices (Ctrl+) and perform multiple actions simultaneously (Ctrl+ to deselect)</li> <li>■ Select multiple links (Ctrl+) and perform multiple actions simultaneously (Shift+ to deselect)</li> <li>■ Filter out unwanted information to facilitate quick access to specific information</li> </ul> <p>The page features two 'modes':</p> <ul style="list-style-type: none"> <li>■ Real Time mode. The page continuously refreshes, presenting up-to-date network information.</li> <li>■ Time Filter. The page presents network information valid for the time defined in a Time Filter but invalid in real time. See <a href="#">Filtering to Access Specific Information</a> on page 147 for information about time filters.</li> </ul>
	Map	<p>The tab's page lets you:</p> <ul style="list-style-type: none"> <li>■ Assess at a glance the enterprise network's global distribution</li> <li>■ Filter</li> </ul> <p>The page features two 'modes':</p> <ul style="list-style-type: none"> <li>■ Real Time mode. The page continuously refreshes, presenting up-to-date network information.</li> <li>■ Time Filter. The page presents network information valid for the time defined in a Time Filter but invalid in real time. See <a href="#">Filtering to Access Specific Information</a> on page 147 for information about time filters.</li> </ul>
	Devices	<p>The tab lets you:</p> <ul style="list-style-type: none"> <li>■ Add a network component:</li> <li>■ Perform a device action</li> <li>■ Show device</li> </ul>
	Links	Lets you add, edit or delete links.
	Sites	<p>Lets you:</p> <ul style="list-style-type: none"> <li>■ add a set of endpoints based on a network subnet</li> <li>■ edit or delete the SIP clients (phones)</li> </ul>

Menu	Tab	Description
	<b>Endpoints</b>	<p>From the tab's drop-down you can select:</p> <ul style="list-style-type: none"> <li>■ Status. Lets you view and monitor the status (Quality of Experience) of phones (for example).</li> <li>■ Configuration. Lets you directly access the Device Manager to configure phones.</li> </ul>
<b>Alarms</b>	<b>Active</b>	Always displays all the active alarms in the network, in real time.
	<b>Journal</b>	Displays only the operator activity alarms in the network.
	<b>History</b>	Displays time frame historical alarms (default), according to the filter.
	<b>Forwarding</b>	For detailed information about forwarding alarms, see <a href="#">Filtering by 'Alarm Names'</a> on page 167.
<b>Statistics</b>	<b>Devices</b>	Displays the Devices Statistics page. Filters on the page allow operators to specify which call quality metrics to display. Quick access to specific information lets operators quickly and effectively maximize users' QoE.
	<b>Links</b>	<p>Displays the Links Statistics page. Filters on the page allow operators to specify</p> <ul style="list-style-type: none"> <li>■ which call quality metrics to display (Successful/Failed Streams, Max Concurrent Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo)</li> <li>■ which links to display (per Topology or Time Range)</li> </ul> <p>Quick access to specific information lets operators quickly and effectively maximize users' QoE.</p>
	<b>Sites</b>	<p>Displays the Sites Statistics page. Filters on the page allow operators to specify</p> <ul style="list-style-type: none"> <li>■ which call quality metrics to display (Successful/Failed Streams, Max Concurrent Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo)</li> <li>■ which sites to display (per Topology or Time Range)</li> </ul> <p>Quick access to specific information lets operators quickly and effectively maximize users' QoE.</p>
	<b>Endpoints</b>	<p>Displays the Endpoints Statistics page. Filters on the page allow operators to specify</p> <ul style="list-style-type: none"> <li>■ which call quality metrics to display (Successful/Failed Streams, Max Concurrent Streams, Streams Quality Utilization Distribution, Avg Call Duration (ACD), MOS, Packet Loss, Jitter, Delay and Echo)</li> <li>■ which endpoints to display (per Topology or Time Range)</li> </ul> <p>Quick access to specific information lets operators quickly and effectively maximize users' QoE.</p>

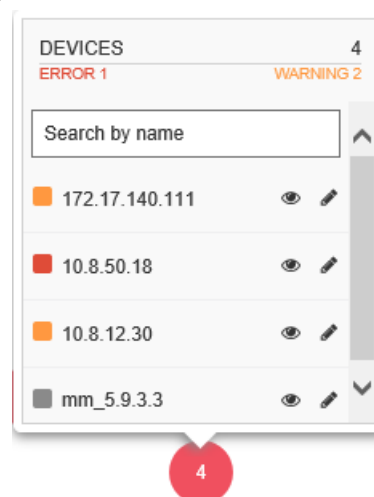
Menu	Tab	Description
	<b>PM Profiles</b>	Facilitates setup of Performance Monitoring capability.
	<b>Reports</b>	Provides operators with essential reports-generation capability which they can utilize to distribute session experience data and comparative analyses quickly and effectively to responsible persons within the enterprise, and to external authorities associated with the enterprise's network, for accurate diagnosis and correction of degraded sessions and for general network optimization. Opens in another Web page.
<b>Calls</b>	<b>Calls List</b>	Displays the Calls List page which presents all the calls made in the enterprise. Filters allow operators to specify which calls to display (Topology, Time Range, Source Type, Quality, etc.). Quick access to specific information allows operators to quickly and effectively maximize users' QoE.
	<b>QoE Thresholds</b>	Lets you apply QoE Threshold profiles for voice quality metrics (MOS, Delay, Packet Loss, Echo and Jitter). A QoE Threshold profile consists of threshold values set for each of these metrics for the 'Poor', 'Fair' and 'Good' call quality categories.
	<b>QoE Status &amp; Alarms</b>	Lets you configure Quality Alarms which are automatically triggered and displayed in the Alarms page if the quality analyzed falls below that defined in the rules. Also lets you determine the status of the voice quality per entity.
<b>Users</b>	<b>Users Experience</b>	Calls Count, Total Duration, Success / Failed, Call Quality, MOS, Jitter, Delay, and Packet Loss. Gives operators network health monitoring capability, including alarms and diagnostics. Used to maximize the quality of experience (QoE) of end users in the network.
	<b>User Details</b>	Displays contact information about the end users: Full Name, User Name, Description, Department, Office, Mobile, Home, MS Skype for Business Line URI, Email, Server, Country. Filters allow quick access to specific users. These filters impact the Users Experience page (see previous), so operators can specify which users whose calls quality of experience they want to assess.
	<b>Active Directories</b>	Lets you add an AD. Displays existing ADs. Allows you to edit and to synchronize with the AD server.
<b>System</b>	<b>Administration</b>	Allows performing administration: <ul style="list-style-type: none"> <li>■ License <ul style="list-style-type: none"> <li>✓ Configuration</li> <li>✓ Tenants Allocations</li> <li>✓ Floating License</li> </ul> </li> <li>■ Security <ul style="list-style-type: none"> <li>✓ Authentication</li> <li>✓ Operators</li> </ul> </li> <li>■ OVOC Server</li> </ul>

Menu	Tab	Description
	<b>Configuration</b>	Allows performing OVOC administration: <ul style="list-style-type: none"> <li>■ Templates (SNMP Connectivity, HTTP Connectivity, QoE Thresholds, QoE Status &amp; Alarms, Perf Monitoring)</li> <li>■ Alarms</li> <li>■ File Manager (Software Manager)</li> <li>■ External Applications</li> <li>■ Device Backup</li> </ul>
	<b>Tasks</b>	Only displays asynchronous actions performed by the OVOC operator.

## Hovering Over a Cluster to Display Information

When more than 200 devices and sites (aggregated) are defined, the Network Topology page will *automatically* be displayed in clusters, reducing clutter and improving operational efficiency. The **Show Clusters** button is displayed only when fewer than 200 devices and sites (aggregated) are defined. When the clusters feature is activated, you can hover over a cluster for this pop-up to be displayed:

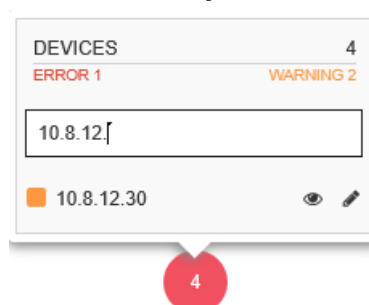
**Figure 2-6: Devices**

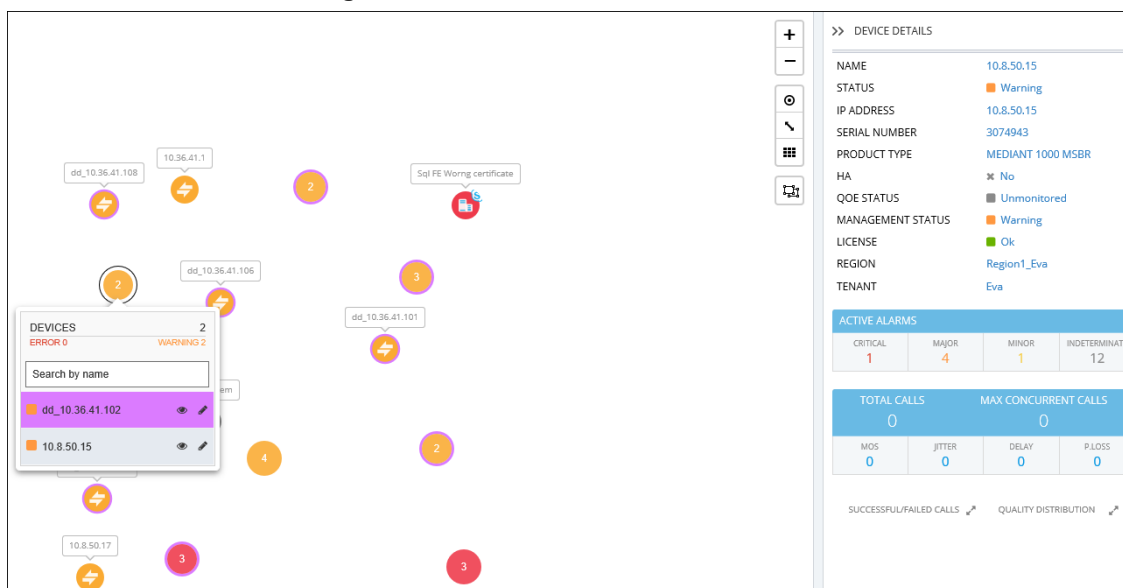


The pop-up indicates the number of errors and warnings in the cluster. The pop-up also displays the entities in the cluster. Click an entity in the list to view information about it in a Device Details pane on the right side of the Network Topology screen (see the Device Details).

The 'Search by name' field enables you to enter the name or - a part of the name - of an entity to search for in the cluster. In large deployments with hundreds of entities, this feature can help operators quickly access a specific entity and view information about it.

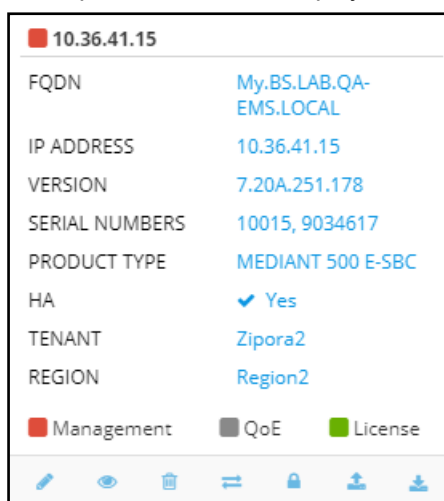
**Figure 2-7: Search by name**



**Figure 2-8: Device Details**

## Hovering Over a Device to Display Information

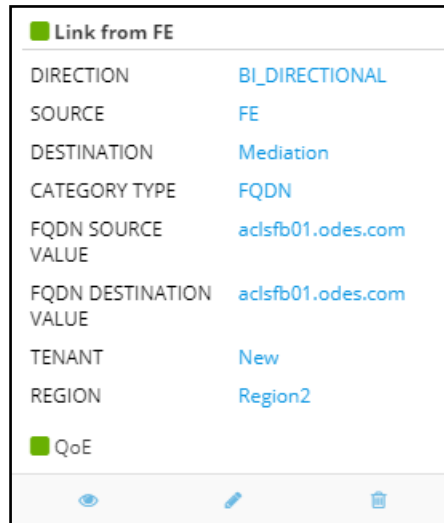
The following figure shows an example of information displayed when hovering over a device.



- The pop-up displays a summary of device information and statuses.
- The lower bar displays icons for actions that can be performed on the device; icons displayed depend on device type.

## Hovering over a Link to Display Information

The following figure shows an example of information displayed when hovering over a link.



- The pop-up displays a summary of link information and statuses.
- The lowermost bar displays icons of actions that can be performed on the link; icons displayed depend on entity type.

## Returning to 'Home' Page by Clicking the AudioCodes Logo

Each page of the OVOC displays the AudioCodes logo in the uppermost left corner:

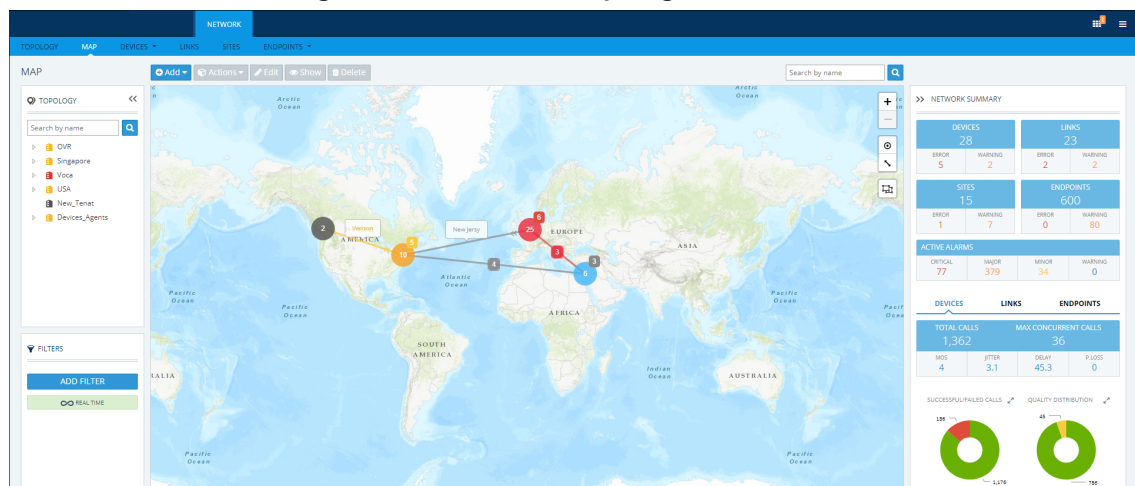


- The logo functions as a 'Home' page button.
- Click it to return to the Network Topology page from any page.
- The feature enhances quick and operator-friendly navigation in the OVOC.

## Getting Acquainted with the Network Map Page





The Network Map page (**Network > Map**) allows operators to determine at a glance the geographical global distribution of the enterprise's IP telephony network.

**Figure 2-9: Network Map Page**



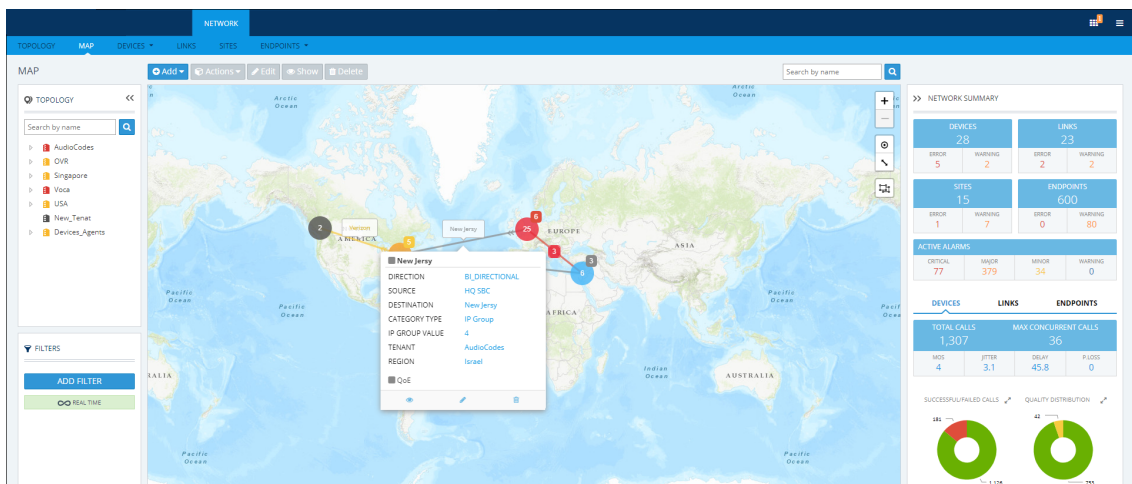
With the exception of cluster icons, entity icons in the Network Map page are identical to those in the Network Topography page described in the table in [Getting Acquainted with the Network Topology Page](#) on page 10. A cluster is based on geographical locations of devices in the Network Map page. Clusters show *aggregated numbers of devices*. Cluster status is unrelated to region and/or tenant status. Region and/or tenant status are only reflected in the Network Map tree and Network Topology tree. Selecting a tenant in the Network Map page's tree impacts the Network Map page in the same way as selecting a tenant in the Network Topology page's tree.

**Table 2-4: Cluster Icons in the Network Map Page**

Cluster Icon	Description
	Cluster status is Error when the status of at least one device or site is Error. Click a cluster to zoom in and view the entities under it.
	Cluster status is Warning when the management status of at least one device or site is Warning. Click a cluster to zoom in and view the entities under it.
	Cluster status is OK when the management status of all devices and sites is OK or Unmonitored. Click a cluster to zoom in and view the entities under it.
	Cluster status is Unmonitored when the management status of all devices and sites is Unmonitored. Click a cluster to zoom in and view the entities under it.

The only difference between Network Map page and the Network Topology page is that in the Network Map page there is no **Show Grid** button. All other buttons are the same. You can hover your cursor over a network entity in the Network Map page to determine its details:

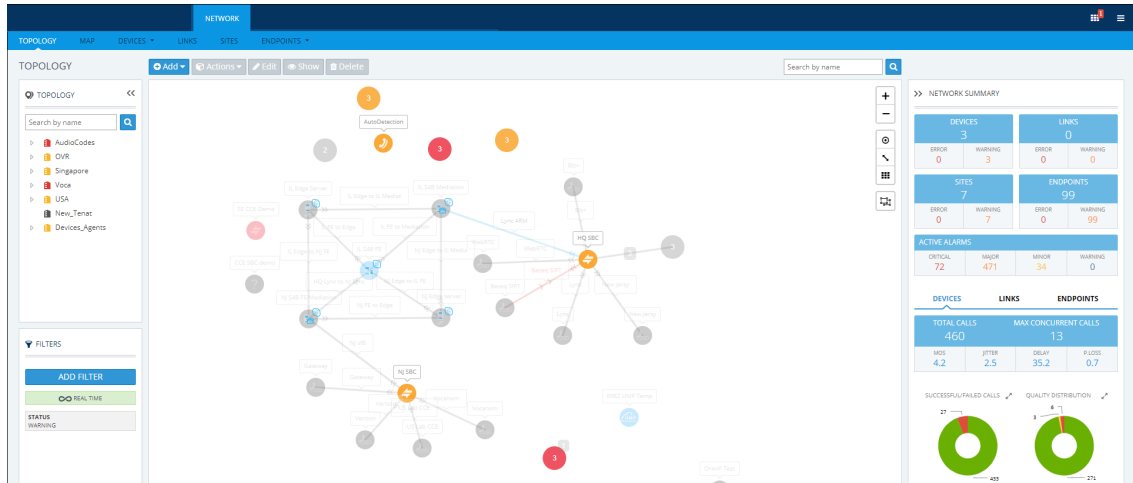
**Figure 2-10: Hovering the Cursor over a Network Entity in the Network Map Page**



In the pane on the right side of the Network Map page, the Network Summary lets you:

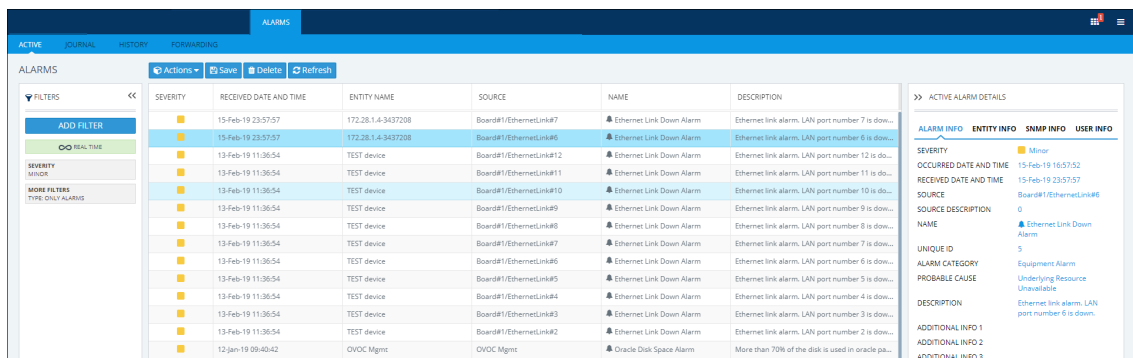
- Determine on how many Devices, Links, Sites and Endpoints, alarms are active.
- Determine which Devices, Links, Sites and Endpoints' status is currently Error / Warning (from the color-coded number). If you click the color-coded number of:
  - **Devices** then the Device Management page opens displaying all devices whose status is Error / Warning
  - **Links** then the Links page opens displaying all links whose status is Error / Warning
  - **Sites** then the Sites page opens displaying all sites whose status is Error / Warning
  - **Endpoints** then the Endpoints page opens displaying all endpoints whose status is Error / Warning

Figure 2-11: Example: Endpoints - 99 Warnings



The Active Alarms pane allows you to determine the total number of Critical, Major, Minor and Indeterminate active alarms (color-coded) currently active in the network. Click any severity level's total to display only alarms of that severity level in the Alarms page. Example: Under **Minor** in the Active Alarms pane above, click **34**:

Figure 2-12: Alarms Filtered by Severity Level

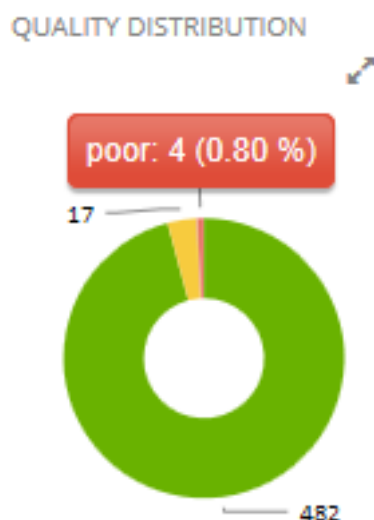


In the Active Alarms pane, you can select an alarm in the page to view detailed information about it in the All Alarm Details pane on the right side of the page.

In the Network Summary window, the **Devices** | **Links** | **Endpoints** tabs display the:

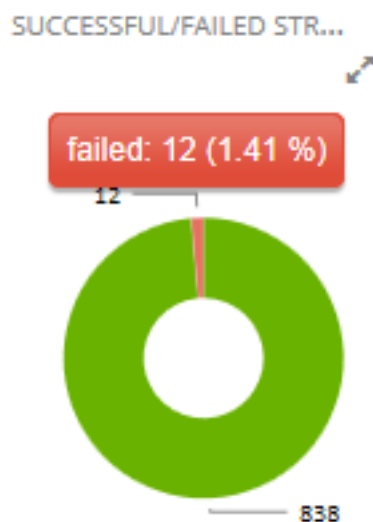
- total # of calls over devices | streams over links | calls over endpoints.
- maximum # of concurrent calls over devices | streams over links.
- average MOS measured over devices | links | endpoints in the network.
- average Jitter measured over devices | links | endpoints in the network.
- average Delay measured over devices | links | endpoints in the network.
- average Packet Loss measured over devices | links | endpoints in the network.

The Quality Distribution pie chart in the Network Summary window allows you to point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of calls over devices | streams over links | calls over endpoints in the network whose quality was measured to be good, fair or poor respectively:



Click any color-coded voice quality segment to open the Calls List filtered by that voice quality score (Good, Fair or Poor).

The Successful/Failed Streams pie chart in the Network Summary window allows you to point your cursor over a green or red segment; a pop-up indicates the # and % of calls over devices | streams over links | calls over endpoints in the network whose performance was measured to be successful or failed respectively:



Click any color-coded segment to open the Calls List filtered by that call performance evaluation (Successful or Failed).

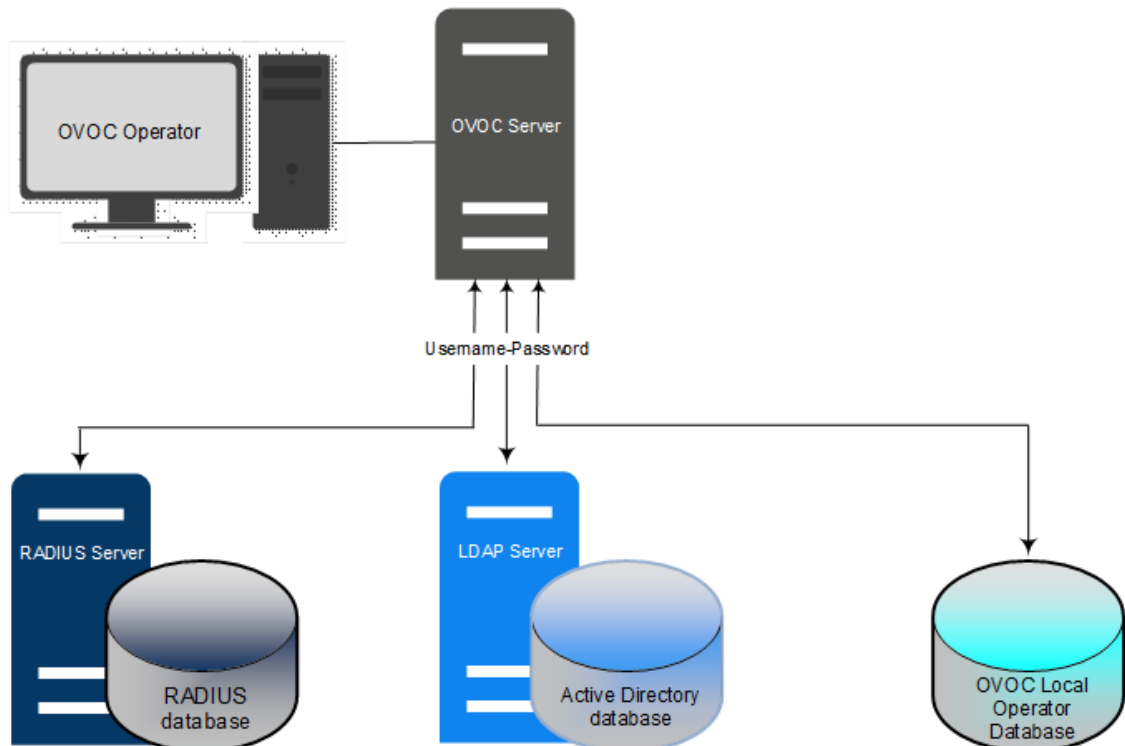
## Configuring Operator Authentication

Authentication of OVOC operators can be configured in three ways:

- Centrally, using an LDAP-compliant server such as Microsoft Active Directory (AD) (see [Configuring Operator Authentication Centrally using an LDAP Server](#) on the next page)
- Centrally, using a RADIUS server (see [Configuring Operator Authentication Centrally with a RADIUS Server](#) on page 31)
- Locally, in the OVOC (see [Configuring Operator Authentication Locally, in the OVOC](#) on page 34)

The following figure shows the three different operator authentication options.

**Figure 2-13: OVOC Operator Authentication Options**



For operator authentication, it's *recommended* to implement a third-party LDAP or RADIUS server in the network. When attempting to log in to the OVOC, the OVOC server then verifies the login username and password with the AD server or RADIUS sever. Usernames, passwords and access-level attributes are stored externally on these platforms. The OVOC server in this case doesn't store the username and password for these users (they're not displayed in the OVOC Users List) but but verifies them with the external authentication server.

## Configuring Operator Authentication Centrally using an LDAP Server

Authentication of OVOC operators can be centrally configured using a Lightweight Directory Access Protocol (LDAP) server. If you already have centralized user authentication via an LDAP server, it's recommended to implement it for OVOC operators as well. When an LDAP-authenticated operator logs into the OVOC, they're assigned one of the OVOC's security levels, e.g., 'Operator'. The equivalent names for these security levels on the LDAP server are shown following. When one of these security levels is not defined on the LDAP server, the OVOC by default allows access to the LDAP-authenticated operator with 'Operator' permissions.

➤ **To centrally configure authentication of OVOC operators using an LDAP server:**

1. In the OVOC, open the Authentication page (**System > Administration > Security > Authentication**).
2. From the 'Authentication Type' drop-down, select **LDAP**.

**Figure 2-14: Authentication - LDAP**

3. Configure the 'LDAP Authentication Server IP'.
4. Configure the 'LDAP Authentication Server Port'.
5. Configure the 'LDAP Connectivity DN' parameter using an Active Directory Service Account (mandatory), for example, **MyServiceAccount@domain**.
6. Configure the 'LDAP Connectivity Password' as required.
7. In the 'LDAP Server Number of Retries' field, enter the number of login attempts the operator can make before they're suspended. When the number is reached, the operator is blocked. Only the 'system' operator whose security level is 'Administrator' can then unblock them. Default: 3 attempts.
8. Configure the 'User DN Search Base' as required.
9. Select the 'SSL' option to secure the connection with the LDAP server over SSL; the 'Certificate' drop-down is activated.
10. From the 'Certificate' drop-down (activated only if 'SSL' is selected), select the certificate file that you want to use to secure the connection with the LDAP server over SSL.
  - **Not selected** (Default). The connection with the LDAP server is non-secured.

- **SSL With Certificate:** An HTTPS connection between the OVOC and the LDAP server is opened. The OVOC authenticates the SSL connection using a certificate. Make sure you load the SSL certificate file, required by the LDAP Active Directory platform, to the Software Manager. See [Adding Configuration Files to the OVOC's Software Manager](#) on page 72.

### Authorization Level Settings



When an operator connects to the OVOC, the OVOC (before allowing the operator access) checks with the LDAP server if the User Group which the operator is associated with in the OVOC, is defined in the LDAP server.

- The parameters below are used to define a User Group in the LDAP server.
- In the Tenant Details screen under the **Multitenancy** tab, the parameter 'LDAP Authentication: Group Name' is used to define a User Group in the OVOC when a tenant level is provisioned (see under [Adding a Tenant](#) on page 85).

If the LDAP validates OVOC's query, the operator is authenticated and allowed access. Operators who are both 'System' and 'Tenant' type are checked in this way. See also [Adding a 'System' Operator](#) on page 37 and [Adding a 'Tenant' Operator](#) on page 43.

11. In the 'System Administrator User Group Name' field, enter the name of the User Group of the 'System' type operator whose security level is 'Administrator'.
12. In the 'System Operator User Group Name' field, enter the name of the User Group of the 'System' type operator whose security level is 'Operator'.
13. In the 'System Monitor User Group Name' field, enter the name of the User Group of the 'System' type operator whose security level is 'Monitor'.
14. In the 'Tenant Administrator User Group Name' field, enter the name of the name of the User Group of the 'Tenant' type operator whose security level is 'Administrator'.
15. In the 'Tenant Operator User Group Name' field, enter the name of the User Group of the 'Tenant' type operator whose security level is 'Operator'.
16. In the 'Tenant Monitor User Group Name' field, enter the name of the name of the User Group of the 'Tenant' type operator whose security level is 'Monitor'.
17. In the 'Tenant Monitor Links User Group Name' field, enter the name of the User Group of the 'Tenant' type operator whose security level is 'Monitor Links'. When an LDAP operator is then assigned to this group, they're logged in as a 'Tenant' type operator with a security level of 'Monitor Links'. Only 'System' type operators can configure this group; 'Tenant' type operators can only view it.
18. From the 'Default Operator Type and Security Level' drop-down, select:

System Administrator
System Operator
System Monitor
Tenant Administrator
Tenant Operator
Tenant Monitor
Tenant Monitor Links

19. Select the **Use LDAP Credentials for Device Page Opening** option for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to the OVOC. The AudioCodes device will then perform authentication with the LDAP server.

20. Under Combined Authentication Mode, select the **Enable combined authentication** option, the 'Authentication Order' drop-down is enabled from which **External First** or **Local First** can be selected.

If **Enable combined authentication** is selected and an operator attempts to log in to the LDAP server but it's unavailable, the OVOC connects to the *local* database with the same operator credentials.

- **External First:** If the LDAP server is unavailable when the LDAP-authenticated operator attempts to log in, the OVOC connects with the same operator credentials to the local (OVOC) operators database.
- **Local First:** If the operator is not found in the local (OVOC) operators database, the OVOC connects with the same operator credentials to the LDAP server.

21. Click **Submit**.

## Configuring Operator Authentication Centrally with a RADIUS Server

You can centrally configure authentication of OVOC operators using a RADIUS (Remote Authentication Dial-In User Service) server. If you already have centralized user authentication via a RADIUS server, it's recommended to implement it for OVOC operators as well.

When the RADIUS-authenticated operator logs into the OVOC, they're assigned one of the OVOC security levels - for example - 'Operator'. If it's not defined on the RADIUS server, the OVOC by default allows access for the RADIUS-authenticated operator, with 'Operator' permission.

### ➤ To centrally configure authentication of OVOC operators using a RADIUS server:

1. Open the Authentication page (**System > Administration > Security > Authentication**) and from the 'Authentication Type' drop-down, select **RADIUS**.

**Figure 2-15: Authentication - RADIUS**

2. Configure the parameters:
  - 'RADIUS retransmit timeout' (Default: 3000 milliseconds). If this timeout expires, local authentication is performed.
  - 'RADIUS auth number of retries' (Default: 1)

Note that these parameters will be used for each RADIUS Server.
3. Select the **Enable display of RADIUS reply message** option. Default: Cleared.
4. From the 'Default Authentication Level' drop-down, select either **Operator** (default), **Amin**, **Monitor** or **Reject**.
5. For each of the three RADIUS servers, define the server's IP address, port and secret. At least one server must be provisioned. 'Server Secret' defines the shared secret (password) for authenticating the device with the server. Must be cryptically strong. Also used by the server to verify authentication of RADIUS messages sent by the device (i.e., message integrity). See the device's manual for more information.
6. Select the **Use RADIUS Credentials for Device Page Opening** option for the OVOC to sign operators in to AudioCodes devices using the same credentials they used to sign in to the OVOC. The AudioCodes device will then perform authentication with the RADIUS server.
7. Under Combined Authentication Mode, select the **Enable combined authentication** option, the 'Authentication Order' drop-down is enabled from which **External First** or **Local First** can be selected.

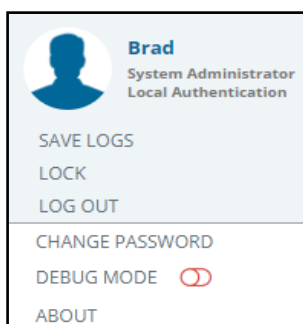
If **Enable combined authentication** is selected and an operator attempts to log in to the RADIUS server but it's unavailable, the OVOC connects to the *local* database with the same operator credentials.

- **External First:** If the RADIUS server is unavailable when the RADIUS-authenticated operator attempts to log in, the OVOC connects with the same operator credentials to the local (OVOC) operators database.
- **Local First:** If the operator is not found in the local (OVOC) operators database, the OVOC connects with the same operator credentials to the RADIUS server.

8. Click **Submit**.

## Viewing Operator Authentication in the Application Information Window

When OVOC operator authentication is performed centrally using an LDAP-compliant server or a RADIUS-compliant server, then after the LDAP-authenticated operator or RADIUS-authenticated operator logs in to the OVOC, the application information window displays the operator's authentication type.



The application information window always displays operator security level irrespective of how authentication is performed.

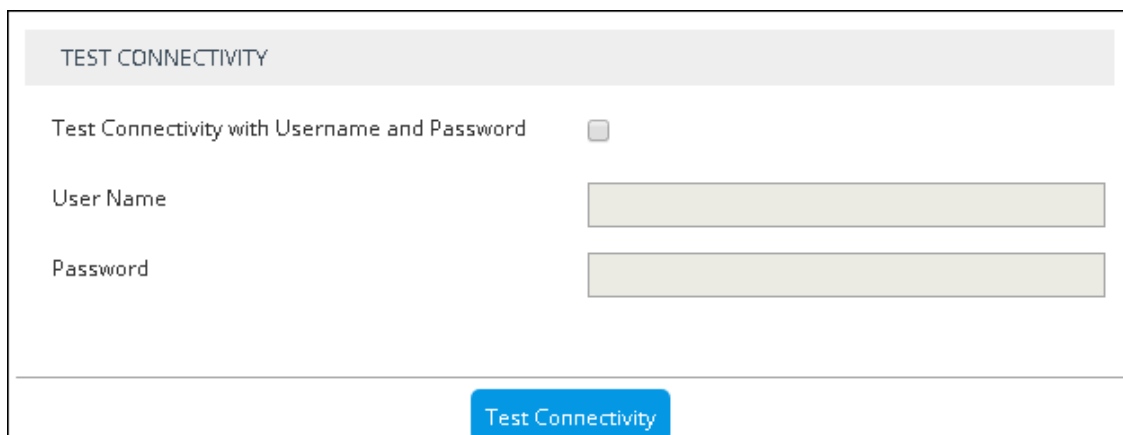
## Testing Connectivity with the LDAP / RADIUS Server

The OVOC allows you to test the settings you configured in the LDAP/RADIUS pages to make sure your configuration is correct and that connectivity with the server has been established.

➤ **To test the settings you configured in the LDAP/RADIUS pages:**

1. In the LDAP or RADIUS authentication page, scroll down to Test Connectivity.

**Figure 2-16: Test Connectivity**



The screenshot shows a web form titled "TEST CONNECTIVITY" in a light gray header. Below the header, there is a checkbox labeled "Test Connectivity with Username and Password". Underneath this checkbox are two text input fields: "User Name" and "Password". At the bottom of the form is a blue button labeled "Test Connectivity".

2. Click **Test Connectivity**; if prompted that the connection was successful, you configured the page correctly; if not, you need to check the settings you configured.
3. [Optional] To test connectivity with a specific operator authentication:
  - Select the option **Test Connectivity with Username and Password** and then enter an operator's name in the 'User Name' field and their password in the 'Password' field.
  - Click **Test Connectivity**; if the operator's credentials are recognized, you're prompted that the connection was successful.

## Configuring Operator Authentication Locally, in the OVOC

You can configure authentication of operators locally, in the OVOC. The feature allows the operator with 'Administrator' security level to control other operators' access to system resources. In this way, sensitive system information cannot be accessed without appropriate authorization, and managed system elements cannot be disrupted by inexperienced operators.

➤ **To locally configure authentication of operators:**

1. In the OVOC, open the Authentication page (**System > Administration > Security > Authentication**).
2. From the 'Authentication Type' drop-down, select **OVOC**.

**Figure 2-17: Authentication – OVOC**

The screenshot displays the 'AUTHENTICATION' configuration page in the OVOC interface. On the left, a sidebar menu shows 'ADMINISTRATION' and 'SECURITY' sections. Under 'SECURITY', 'Authentication' is highlighted. The main content area shows 'Authentication Type' set to 'OVOC'. Below this, the 'OVOC AUTHENTICATION SETTINGS' are listed with input fields for various parameters:

- Number of login attempts before blocking: 5
- Max number of simultaneous login sessions: 5
- Display Duration (Seconds) for Notifications: 3
- Minimum password length: 8
- Non repetitive characters from previous password: 0
- Password complexity rules: No Complexity Rules
- Number of not reused previous passwords: 5
- Dictionary check for password cracking simplicity: ☐
- Enable password expiration extension: ☐
- Number of additional logins (after password expired): 1
- Additional logins time period (days): 1

A 'Submit' button is located at the bottom right of the settings area.

3. Configure the authentication parameters using the following table as reference.

**Table 2-5: OVOC Authentication Parameters**

Parameter	Description
Number of login attempts before blocking	Lets you configure the number of login attempts attempted by the operator before the OVOC application blocks them. When the number of login attempts is reached, the operator is blocked from logging into the OVOC. Only the Administrator can then unblock the suspended operator. Default: 3 attempts.
Max number of simultaneous login sessions	Lets you configure up to how many operator login sessions can be performed simultaneously. Default: 5

Parameter	Description
Notifications display time (sec)	Lets you configure for how long (in seconds) the notifications pop-up window is displayed after performing tasks such as adding a device or when alarms are received. Default: 3 seconds. Setting the parameter to 0 prevents notifications from being displayed. All notifications are cleared from the OVOC server after twenty minutes. See also <a href="#">Forwarding Alarms whose Destination Type is 'Notification'</a> on page 181.
Minimum password length	Default: 8 characters. Maximum supported: 30 characters.
Non repetitive characters # from previous password	Default: 0. Maximum supported: 10 characters.
Password complexity rules	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ No complexity rules are applied (default)</li> <li>■ Use Plain or Capital letters, Digits and Special Characters</li> <li>■ Use Plain and Capital letters, Digits and Special Characters</li> </ul>
Number of not reused previous passwords	Default: 5. Possible values: 0-10.
Dictionary check for password cracking simplicity	Select this option for the OVOC server to perform a password weakness check on the OVOC operator's password. Default: Disabled (unselected).
Enable Password Expiration Extension	Select the option to extend the password expiration; the following two parameters are activated.
Number of Additional Logins (after Password Expired)	Defines the number of logins operators can perform after their password expires. Range: 1-10.
Additional Logins Time Period (days)	Defines the period (in days) during which the operator can perform the number of additional logins defined with the previous parameter. Range: 1-60.

## Adding an Operator

You can add an operator to the OVOC. The operator can be of type:

- 'Tenant' - or-
- 'System'

The following table shows the capabilities permitted for each OVOC operator type and security level. OVOC operators are allocated a security level of either Admin, Operator or Monitoring.

**Table 2-6: Capabilities Allowed for Each Operator Type / Security Level**

Op Type	Security Level	Define ops	Manage tenants	Manage system resources	Manage tenant resources	Monitor system resources	Monitor tenant resources
System	Admin	Yes, all op types and security levels	Yes	Yes	Yes	Yes	Yes
	Operator	No	No	Yes	Yes	Yes	Yes
	Monitor	No	No	No	No	Yes	Yes
Tenant	Admin	Yes, in their own 'tenant'	No	No	Yes, in their own 'tenant'	No	Yes
	Operator	No	No	No	Yes, in their own 'tenant'	No	Yes
	Monitor	No	No	No	No	No	Yes
	Tenant Monitor Links	No	No	No	No	No	Links only

## How Multi Tenancy Impacts Operator Capabilities

The impact of multi tenancy architecture on the capabilities of OVOC 'system' operators is different to its impact on OVOC 'tenant' operators.

Here are some examples that will help you deduce the principle. Use the table shown in [Adding an Operator](#) above as reference. Examples also show how operator security level impacts the capabilities of 'system' operators and 'tenant' operators.

- A 'system' operator with a security level of 'Admin' will be permitted *every capability*.
- A 'tenant' operator with a security level of 'Monitoring' will *not be permitted any capability* except to monitor their own resources.
- In the OVOC's Software Manager:
  - A 'system' operator can add | delete files.
  - A 'tenant' operator can only *use* files.

- A 'tenant' operator with Admin security level, however, can add | delete files *if the files only belong to that specific tenant and only devices in that tenant use them.*
- A 'system' operator with Admin security level can allocate licenses to tenants.  
A 'tenant' operator with Admin security level can only *distribute sessions within their own tenant*, across *that tenant's* devices, from *that tenant's* License Pool. A 'tenant' operator *cannot manage licenses for multiple tenants* like a 'system' operator with Admin security level can.
- Multi-Tenancy impacts what operators view on OVOC pages. In the Network Topology page, for example:
  - a 'tenant' operator with a Monitoring security level will only see part of the network.
  - A 'tenant' operator with Admin security level will only see network entities they are permitted to see.
  - A 'system' operator with an Admin security level will see all tenants and all devices under each tenant.

## Adding a 'System' Operator

You need to add a 'system' operator to the OVOC. The 'system' operator is typically the ITSP administrator whose network features multi-tenancy architecture and whose OVOC application provides management services to multiple enterprise customers (tenants) in their network. The 'system' operator can also be an *enterprise network administrator* whose network does *not* feature multi-tenancy architecture but whose OVOC application enables management of the enterprise's *distributed offices* ('tenants').



Only a 'system' operator with a security level of 'Admin' can perform tenant management operations (Add/Remove/Update).

### ➤ To add a 'system' operator:

1. In the OVOC, open the Operators page (**System > Administration > Security > Operators**).
2. Click **Add** and then select **System Operator** from the drop-down menu.

**Figure 2-18: 'System' Operator Settings - Basic Info**

SYSTEM OPERATOR DETAILS

**BASIC INFO** **ADVANCED INFO**

Change Password on Next Login ☐

Operator Name \*

Password \*

Confirm Password \*

Operator Type System

Security Level Monitoring

Valid IPs to Login From

Full Name

Phone

Email

Description

OK Close

- Configure the new operator's basic information using the following table as reference. The screen displays basic operator information and security settings.

**Table 2-7: 'System' Operator Settings - Basic Info**

Parameter	Description
User Name	Enter the operator's name. Must be unique.
Password	Enter the operator's password.
Confirm Password	Confirm the operator's password.
User Type	[Read-only] <b>System</b> or <b>Tenant</b> depending on what you selected in step 2.
Security Level	From the drop-down select: <ul style="list-style-type: none"> <li>Monitoring (lowest security level)</li> <li>Operator (medium security level)</li> <li>Admin (highest security level)</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>■ Monitoring Links (Applicable only when adding a 'Tenant' type operator in a deployment whose architecture is ITSP customer multi-tenant architecture - see <a href="#">ITSP Customer Multi-Tenant Architecture</a> on page 5. When adding this operator to links, all links must have the same source SBC - except when using LDAP authentication - and the links' source and destination devices must be in the operator's tenant. Only SBC device links are supported; Skype, SmartTAP, UMP and CloudBond links are not supported. The operator will only be able to monitor information related to QoE (calls, statistics and link alarms).</li> </ul>
Valid IPs to Login From	Enter IP addresses of devices from which this operator will be allowed to log in. Login from any other IP address will be disallowed.
Full Name	Enter the operator's full name. Facilitates more effective management of operators.
Phone	Enter the operator's phone number. Facilitates more effective management of operators.
Email	Enter the operator's email. Facilitates more effective management of operators.
Description	Enter any information likely to facilitate more effective management of OVOC operators.

4. Click **Advanced Info**.

**Figure 2-19: 'System' Operator Settings – Advanced Info**

**SYSTEM OPERATOR DETAILS** [X]

**BASIC INFO** **ADVANCED INFO**

Suspend User ☐

Suspension Reason

Account Inactivity Period (Days)

Session Timeout Period (Minutes)

Session Leasing Period (Hours)

Password Update Min Period (Hours)

Password Validity Max Period (Days)

Password Warning Max Period (Days)

Allowed Login Attempts

**OK** **Close**

5. Configure the new 'system' operator's advanced information using the following table as reference. The screen displays advanced account and password settings.

**Table 2-8: 'System' Operator Settings – Advanced Info**

Parameter	Description
Suspend User	Select this option to suspend the 'system' operator.
Suspension Reason	[Only available when 'Suspend User' is checked] Enter a reason explaining why the operator is suspended.
Suspension Time	[Only available when 'Suspend User' is checked] Enter the time at which the operator is suspended.
Account Inactivity Period (Days)	If the operator does not log into the OVOC for the number of days specified, their account will be suspended. Maximum: 10 days. Default: 0 (The operator can log into the OVOC at any time irrespective of how long they've been logged off; even if they haven't logged in for an excessive period of time their account will not be suspended).

Parameter	Description
Session Inactivity Period (Minutes)	Defines how long an OVOC GUI page remains accessible despite operator inactivity. If the period times out, the page locks and the operator is prompted to reenter their password to re-access it; the same page that the operator was on before the period timed out then opens. After the operator logs in to the GUI, every time they interact with it, e.g., by clicking a menu, the timer is reset. Default: 0 (the GUI is always accessible irrespective of operator inactivity).
Session Leasing Duration (Hours)	Enter the session leasing duration, in hours. If it expires, the application will close the client session / force the operator to reenter their password in order to re-access the application. Default: 0 (the session leasing duration will never expire and the application will never close the client session). Note that the Device Manager inherits the value configured.
Password Update Min Period (Hours)	Specify a period, in hours. The operator's password cannot be changed more than once within the period specified. Default: 24 hours. If 0 is specified, the password can be changed an unlimited number of times, unrestricted by period.
Password Validity Max Period (Days)	Specify a period, in days. The operator's password must be changed within this number of days after the last password change. Default: 90 days. If 0 is specified, the password can be changed an unlimited number of times, unrestricted by period, after the last password change.
Password Warning Max Period (Days)	Specify the number of days. The operator will receive a warning message this number of days before the date on which the password expires. Default: 7 days (i.e., the operator will receive a warning message a week before their password expires). If 0 is specified, the operator will receive warning messages irrespective of the date on which the password expires.
Allowed Login Attempts	Provides the capability to define the number of login attempts the operator can make before they're suspended, per operator. Enhances operator security management.

- Click **OK**. The operator is added to the OVOC.

## Editing a 'System' Operator

You can edit the details of a 'system' operator if they change.

➤ **To edit the details of a 'system' operator:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the 'system' operator whose details you need to edit and then click **Edit**; the Operator Settings screen opens.
3. Edit the operator's details using the table as reference.

## Deleting a 'System' Operator

You can remove a 'system' operator from the OVOC.

➤ **To remove a 'system' operator:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the 'system' operator to remove and then click **Delete**.

## Deleting Multiple Operators

You can delete multiple operators from the OVOC simultaneously.

➤ **To delete multiple 'system' operators simultaneously:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the operators to remove and then click **Delete**.

## Suspending a 'System' Operator

You can suspend a 'system' operator from the OVOC.

➤ **To suspend a 'system' operator:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the 'system' operator to suspend and then click **Actions**.
3. From the drop-down, select **Suspend**; the operator is automatically logged out before suspension.

## Releasing a Suspended 'System' Operator

You can release a 'system' operator who was previously suspended from the OVOC.

➤ **To release an operator who was previously suspended from the OVOC:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the suspended operator to release and then click **Actions**. Multiple operators can be selected for release from suspension.
3. From the drop-down, select **Release**.

## Forcing a Password Change

You can force an operator to change their password. The feature can be used if for example you suspect information has been stolen from the enterprise.

➤ **To force a password change:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the operator whose password to change and then click **Actions**. Multiple operators can be selected.
3. From the drop-down, select **Force Password Change**.



The operator is automatically prompted to change their password the next time they log in.

## Forcing an Operator Logout



Applies only to OVOC operators with 'Admin' security level. See [Adding an Operator](#) on page 36 for an explanation of the different security levels.

An OVOC operator with 'Admin' security level can force an active operator to be logged out, conforming to established management application standards. The operator with 'Admin' security level may (for example) need to urgently remove an active operator before another mistake is made and more damage is done.

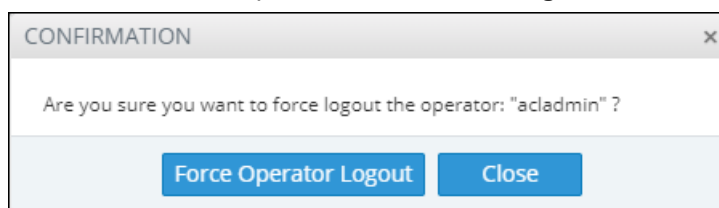
- **To force an active operator to be logged out:**

1. Open the Operators page (**System > Administration > Security > Operators**).

**Figure 2-20: Operators page**

OPERATORS															
		<div><div><div><div></div><div>Add</div></div><div><div></div><div>Edit</div></div><div><div></div><div>Actions</div></div><div><div></div><div>Delete</div></div></div></div>													
ADMINISTRATION <<		OPERATOR NAME		FORCE LOGOUT		SECURITY LEVEL		STATUS		LAST SUCCESSFUL LOGIN		LAST FAILED LOGIN		>> OPERATOR DETAILS	
				SUSPEND											
		actadmin		FORCE PASSWORD CHANGE		ADMIN		ACTIVE		04-Feb-19 11:01:36					
LICENSE		Operator		System		OPERATOR		NOT ACTIVE		09-Jan-19 07:55:58				OPERATOR NAME actadmin	
Configuration		Monitor		System		MONITORING		NOT ACTIVE		15-Jan-19 13:06:20				OPERATOR TYPE System	
Tenants Allocations		Zip_Admin		Tenant		ADMIN		NOT ACTIVE		09-Jan-19 08:01:48				SECURITY LEVEL ADMIN	
Floating License		Zip_Operator		Tenant		OPERATOR		NOT ACTIVE		09-Jan-19 08:13:21				VALID IPS TO LOGIN FROM	
SECURITY		Zip_Monitor		Tenant		MONITORING		NOT ACTIVE		09-Jan-19 08:14:40				FULL NAME	
Authentication		New_Admin		Tenant		ADMIN		NOT ACTIVE		15-Jan-19 09:18:09				PHONE	
Operators		NewOperator		System		ADMIN		NOT ACTIVE						DESCRIPTION	
OVOC SERVER		SysAdmin		System		ADMIN		NOT ACTIVE		04-Dec-18 10:21:09				IS SUSPENDED X	
														SUSPENSION REASON	

2. Select the active operator to log out; their 'Active' status is indicated in the Status column.
3. From the now enabled 'Actions' drop-down, select **Force Logout**.



- Click **Force Operator Logout** to implement the action.

## Adding a 'Tenant' Operator

You can add a 'tenant' operator to the OVOC. A 'tenant' operator is typically an enterprise's network administrator whose network does not feature multi-tenancy architecture and whose OVOC application enables management of the enterprise's distributed offices.



Only a 'system' operator with a security level of 'Admin' can perform 'tenant' management operations (Add/Remove/Update/Clone/Suspend.

➤ To add a 'tenant' operator:

1. In the OVOC, open the Operators page (**System > Administration > Security > Operators**).
2. Click **Add** and then select **Tenant Operator** from the drop-down menu.

**Figure 2-21: 'Tenant' Operator Details – Basic Info**

TENANT OPERATOR DETAILS

**BASIC INFO**      **ADVANCED INFO**      **TOPOLOGY**

Change Password on Next Login ☐

Operator Name \*

Password \*

Confirm Password \*

Operator Type Tenant

Security Level Monitoring

Valid IPs to Login From

Full Name

Phone

Email

Description

OK Close

3. Configure the 'tenant' operator's basic info using the table 'System Operator Settings – Advanced Info' as reference.
4. Click **Advanced Info**.

**Figure 2-22: 'Tenant' Operator Details – Advanced Info**

The screenshot shows a web-based configuration window titled "TENANT DETAILS". It has a tabbed interface with five tabs: "GENERAL", "SNMP", "HTTP", "MULTITENANCY", and "LICENSE". The "GENERAL" tab is currently selected. Inside this tab, there are five input fields: "Tenant Name \*" (a text box), "Is Default" (a dropdown menu showing "False"), "License Pool Operator" (a dropdown menu), "Description" (a text box), and "Subnet (CIDR Notation)" (a dropdown menu). At the bottom of the window, there are two buttons: "OK" and "Close".

- Configure the 'tenant' operator's advanced information using the following table as reference. The screen displays advanced account and password settings.

**Table 2-9: 'Tenant' Operator Settings – Advanced Info**

Parameter	Description
Suspend User	Select this option to suspend the 'system' operator.
Suspension Reason	[Only available when 'Suspend User' is checked] Enter a reason explaining why the operator is being suspended.
Suspension Time	[Only available when 'Suspend User' is checked] Enter the time at which the operator is being suspended.
Account Inactivity Period (Days)	If the operator does not log into the OVOC for the number of days specified, their account will be suspended. Maximum: 10 days. Default: 0.
Session Inactivity Period (Minutes)	Enter the session inactivity period, in minutes. If it expires, the application will close the client session / force the operator to reenter their password in order to reaccess the application. Default: 0.
Session Leasing Duration (Hours)	Enter the session leasing duration, in hours. If it expires, the application will close the client session / force the operator to reenter their password in order to reaccess the application. Default: 0.

Parameter	Description
Password Update Min Period (Hours)	Specify a period, in hours. The operator's password cannot be changed more than once within the period specified. Default: 24 hours.
Password Validity Max Period (Days)	Specify a period, in days. The operator's password must be changed within this number of days after the last password change. Default: 90 days.
Password Warning Max Period (Days)	Specify the number of days. The operator will receive a warning this number of days before the date on which the password expires. Default: 7 days (i.e., the operator will receive a warning message a week before their password expires).
Allowed Login Attempts	Provides the capability to define the number of login attempts the operator can make before they're suspended, per operator. Enhances operator security management.

6. Click **Tenants**.

**Figure 2-23: 'Tenant' Operator Settings – Tenants**

7. [The screen is only available for the 'tenant' operator]. From the 'Assigned Tenant' drop-down, select a tenant for this operator from the list of tenants defined in the server. Multiple tenants can be selected.

**Figure 2-24: 'Tenant' Operator Settings – Tenant Assigned**

The screenshot shows a window titled "TENANT OPERATOR DETAILS" with a close button (X) in the top right corner. Below the title bar are three tabs: "BASIC INFO", "ADVANCED INFO", and "TENANTS". The "TENANTS" tab is selected and highlighted with a blue underline. Inside the "TENANTS" tab, there is a label "Assigned Tenants:" followed by a list box. The list box contains one item, "floating\_license", which has a small blue 'X' icon to its right. Below the list box is a vertical line indicating where to click to add more tenants. At the bottom of the dialog, there are two buttons: "OK" and "Close".

8. Click **OK**; the tenant/s is/are assigned.

## Editing a 'Tenant' Operator

You can edit the details of a 'tenant' operator if they change.

### ➤ To edit the details of a 'tenant' operator:

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the 'tenant' operator whose details you need to edit and then click **Edit**; the Operator Settings screen opens.
3. Edit the operator's details using the table describing the 'tenant' operator's advanced information as reference.

## Deleting a 'Tenant' Operator

You can remove a 'tenant' operator from the OVOC. After removal, the OVOC deletes the 'tenant' operator's entities, frees its portion of license resource, and detaches any operator attached to it.

### ➤ To remove a 'tenant' operator:

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the 'tenant' operator to remove and then click **Delete**.

## Deleting Multiple Operators

You can delete multiple operators from the OVOC simultaneously. After deleting, the OVOC deletes the operators' entities, frees their portion of license resource, and detaches any attached operators.

➤ **To delete multiple operators simultaneously:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the operators to remove and then click **Delete**.

## Suspending a 'Tenant' Operator

You can suspend a 'tenant' operator from the OVOC.

➤ **To suspend a 'tenant' operator:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the 'tenant' operator to suspend and then click **Actions**. Multiple operators can be selected for release from suspension.
3. From the drop-down, select **Suspend**; the operator is automatically logged out before suspension.

## Releasing a Suspended 'Tenant' Operator

You can release a 'system' operator who was previously suspended from the OVOC.

➤ **To release an operator who was previously suspended from the OVOC:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the suspended operator to release and then click **Actions**.
3. From the drop-down, select **Release**.

## Forcing a Password Change

You can force an operator to change their password. The feature can be used if for example you suspect information has been stolen from the enterprise.

➤ **To force a password change:**

1. Open the Operators page (**System > Administration > Security > Operators**).
2. Select the operator whose password to change and then click **Actions**. Multiple operators can be selected.
3. From the drop-down, select **Force Password Change**.



The operator is automatically prompted to change their password the next time they log in.

## Forcing an Operator Logout



Applies only to OVOC operators with 'Admin' security level. See [Adding an Operator](#) on page 36 for an explanation of the different security levels.

An OVOC operator with 'Admin' security level can force an active operator to be logged out, conforming to established management application standards. The operator with 'Admin' security level may (for example) need to urgently remove an active operator before another mistake is made and more damage is done.

- **To force an active operator to be logged out:**

1. Open the Operators page (**System > Administration > Security > Operators**).

**Figure 2-25: Operators page**

[illegible]

2. Select the active operator to log out; their 'Active' status is indicated in the Status column.
3. From the now enabled 'Actions' drop-down, select **Force Logout**.

CONFIRMATION

Are you sure you want to force logout the operator: "acladmin" ?

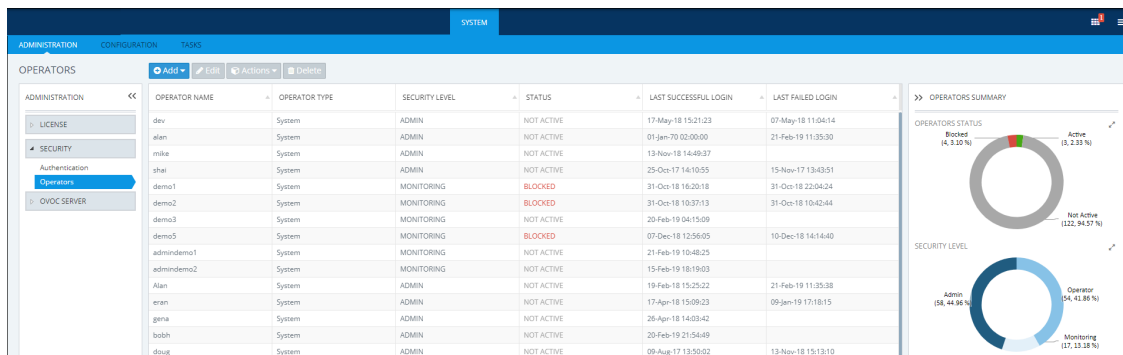
Force Operator Logout

Close

4. Click **Force Operator Logout** to implement the action.

### 3 Configuring Global (System) Settings

After logging in, configuring operator authentication and then adding an operator, you can configure the settings under the OVOC's System menu. These are the OVOC's *global* settings. They are *system-wide*, as opposed to *per tenant*.



Three tabs are displayed under the System menu: **Administration**, **Configuration** and **Tasks**. The following table describes the tabs, folders and items under the System menu.

**Table 3-1: System Menu**

Tab	Folder	Item	Description
Administration	License	Configuration	See <a href="#">Making Sure your License Provides the Capabilities you Ordered</a> on page 52 for details.
		Tenants Allocation	See <a href="#">Allocating Licenses to Tenants</a> on page 53 for details.
		Floating License	See under <a href="#">Managing SBC Licenses</a> on page 122 for details.
	Security	Authentication	Lets you configure LDAP/RADIUS authentication. See <a href="#">Configuring Operator Authentication</a> on page 27 for details.
		Operators	Lets you add operators to the OVOC. See <a href="#">Adding an Operator</a> on page 36 for details.
	OVOC Server	Status	Lets you view information about the status of the OVOC server
		Info	Lets you view information about the OVOC server
		Configuration	Lets you configure the general OVOC server settings. See <a href="#">Securing Connections with FQDN or IP Address</a> on page 57.

Tab	Folder	Item	Description
Configuration	Templates	SNMP Connectivity	See <a href="#">SNMP Connectivity</a> on page 63 for details.
		HTTP Connectivity	See <a href="#">HTTP Connectivity</a> on page 65 for details.
		QoE Thresholds	See <a href="#">QoE Thresholds</a> on page 65 for details.
		QoE Status & Alarms	See <a href="#">QoE Status and Alarms</a> on page 67 for details.
		Perf Monitoring	See <a href="#">Adding a PM Profile</a> on page 193 for details.
	Alarms		See <a href="#">Configuring Alarms Settings</a> on page 69 for details.
	File Manager	Software Manager	See <a href="#">Adding Configuration Files to the OVOC's Software Manager</a> on page 72 for details.
External Applications			See <a href="#">Connecting Directly to External Applications</a> on page 76 for details.
Device Backup			See <a href="#">Enabling Automatic Device Backup Periodically</a> on page 80 for details.
Tasks			See <a href="#">Tasks tab</a> on page 81 for details.

## Administration tab

Under the **Administration** tab's **License** folder you can view a summary of your license and allocate licenses to tenants. See [Making Sure your License Provides the Capabilities you Ordered](#) on the next page for more information.

Under the **Administration** tab's **Security** folder you can define authentication and add operators. See [Allocating Licenses to Tenants](#) on page 53 for more information.

## Loading the OVOC Server License

Before Version 7.6.1000, the OVOC Server License could only be loaded to the server using the EMS Server Manager, described in the *One Voice Operations Center IOM Manual*. For operators' convenience, the OVOC Server License as of Version 7.6.1000 can also be loaded from the OVOC GUI to the OVOC server after it is obtained as a file from AudioCodes.



Only a 'System' type operator whose security level is defined as 'Admin' can load the OVOC server license. See [Adding an Operator](#) on page 36 for more information.

### ➤ To load the license:

1. Open the License Configuration page (**System > Administration > License > Configuration**).

**Figure 3-1: License Configuration**

2. Click the **Load License** button and in the browser window that opens, navigate to the txt file containing the license on your machine.
3. Click **Open** for the load to be performed.



- The license is provided without installation media. To activate the product, follow the activation instructions described in the *One Voice Operations Center IOM Manual*.
- The Alarms Journal displays the Load License action as a server action. The Alarms Journal also displays the values of the new license and the name of the operator who performed the action.

## Making Sure your License Provides the Capabilities you Ordered

The License Configuration page allows you to view the details of the capabilities which the license that you ordered covers. Use the page to make sure the license you purchased provides the capabilities you ordered.

### ➤ To view the details of your license:

1. Open the License Configuration page (**System > Administration > License > Configuration**).

**Figure 3-2: License Configuration**

**LICENSE CONFIGURATION** [Load License](#)

**ADMINISTRATION** <<

- LICENSE**
  - Configuration**
  - Tenants Allocations
  - Floating License
- SECURITY
- OVOC SERVER

**GENERAL**

Machine ID: 9E4F378BA192 Reason:   
 Product Key: UA4C6E671FF02XH6 Expiration Date: 01-01-2020   
 Status: Enable Expiration Days Left: 329

**FLOATING LICENSE**

Status: Enable

**LICENSE POOL**

**Managed Devices** 0%   
 Total: 1,000,000 Allocated: 1,050 Free: 998,950

**SBC License Pool**

**SBC Sessions** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**SBC Transcoding** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**SBC Registrations** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**SBC Signaling** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**CloudBond License Pool**

**CB PBX Users** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**CB Users** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**CB Voicemail Accounts** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**CB Analog Devices** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**VOICE QUALITY**

**Users** 0%   
 Total: 1,000,000 Allocated: 2,000 Free: 998,000

**Devices** 0%   
 Total: 1,000,000 Allocated: 1,100 Free: 998,900

**Sessions** 0%   
 Total: 1,000,000 Allocated: 1,100 Free: 998,900

**Endpoints** 1%   
 Total: 1,000,000 Allocated: 10,100 Free: 989,900



The License Configuration page displays only the parameters that exist in the License Key provided by AudioCodes.

2. Make sure the license you purchased provides the capabilities you ordered.

## Allocating Licenses to Tenants

After adding tenants as described in [Adding a Tenant](#) on page 85, you can allocate licenses to them manually if your network administrator changed the default dynamic automatic allocation (see [Dynamic Allocation of Endpoint Licenses](#) on page 119). The Tenants Allocation page lets you manually allocate licenses to tenants.

### ➤ To allocate licenses to tenants:

1. Open the Tenants Allocations page (**System > Administration > License > Tenants Allocations**).

### Figure 3-3: Tenants Allocations

TENANTS ALLOCATIONS														
ADMINISTRATION	TENANT	MANAGED DEVICES	SBC SESSIONS	SBC REGISTRATIONS	SBC TRANSCODING	SBC SIGNALING	CB USERS	CB PBX USERS	CB ANALOG DEVICES	CB VOICEMAIL ACCOUNTS	QOE DEVICES	QOE ENDPOINTS	QOE SESSIONS	QOE USERS
LICENSE	Elishewa	50	50	50	50	500	5,000	5,000	0	5,000	10,000	1,000	10,000	10,000
Summary	tt	50,000	50,000	50,000	5,000	50,000	50,000	5,000	5,000	5,000	5	50,000	5	10,000
<div>Tenants Allocations</div> <div>Floating License</div>														
SECURITY														
OVOC SERVER														

2. Select the tenant to whom to allocate licenses and then click **Edit**.

### Figure 3-4: Tenant Allocations Details

**TENANT ALLOCATIONS DETAILS**

**LICENSE POOL**

Resource	Value	Total	Allocated	Free
Managed Devices:	50	1,000,000	50,052	949,948
SBC Sessions:	50	1,000,000	50,052	949,948
SBC Registrations:	50	1,000,000	50,052	949,948
SBC Transcoding:	50	1,000,000	5,052	994,948
SBC Signaling:	500	1,000,000	50,500	949,500
CB Users:	5000	1,000,000	55,002	944,998
CB PBX Users:	5000	1,000,000	55,002	944,998

OK Close

**TENANT ALLOCATIONS DETAILS**

CB Voicemail Accounts:  Total: 1,000,000 Allocated: 10,000 Free: 990,000 1%

**VOICE QUALITY**

Devices:  Total: 1,000,000 Allocated: 15,000 Free: 985,000 2%

Endpoints:  Total: 1,000,000 Allocated: 1,060 Free: 998,940 0%

Sessions:  Total: 1,000,000 Allocated: 60,000 Free: 940,000 6%

Users:  Total: 1,000,000 Allocated: 10,055 Free: 989,945 1%

**ENDPOINTS MANAGEMENT**

Endpoints:  Total: 1,000,000 Allocated: 1,060 Free: 998,940 0%

OK Close



Only parameters in the License Key provided by AudioCodes are displayed.

3. In the Tenant Allocations Settings shown in the figures above, you can allocate:

- **Under Fixed License Pool**
  - ◆ CB analog devices
  - ◆ CB PBX users
  - ◆ CB user sessions
  - ◆ CB voicemail accounts
  - ◆ SBC Registrations (SIP endpoints that can register with the SBC)
  - ◆ SBC sessions (media and signaling)
  - ◆ SBC Signaling sessions
  - ◆ SBC Transcoding sessions
- **Under Voice Quality**
  - ◆ Devices
  - ◆ Endpoints
  - ◆ Sessions
  - ◆ Users
- **Under Endpoints Management**
  - ◆ Endpoints

## Authenticating Operators

The 'Security' folder's **Authentication** item lets you configure LDAP and RADIUS authentication. See [Configuring Operator Authentication](#) on page 27 for detailed information.

The 'Security' folder's **Operators** item lets you add OVOC operators. See [Adding an Operator](#) on page 36 for detailed information.

## Determining OVOC Server Status

The Server Status page (**System > Administration > OVOC Server > Status**) lets you determine at-a-glance status information about the OVOC server, including processes status and open ports status. The feature saves operators from having to log in to the EMS Server Manager. The same information is presented, only in friendlier format.

**Figure 3-5: Server Status page**

SERVER STATUS		Refresh
ADMINISTRATION <<		
<div>LICENSE</div> <div>Configuration</div> <div>Tenants Allocations</div> <div>Floating License</div>		
<div>SECURITY</div> <div>Authentication</div> <div>Operators</div>		
<div>OVOC SERVER</div> <div>Status</div> <div>Info</div> <div>Configuration</div>		
PROCESSES STATUS		
Watchdog	■	OVOC ■
QoE CPEs	■	QoE Lync ■
QoE Endpoints	■	NTP Daemon ■
Oracle DB	■	Oracle DB Listener ■
Cassandra DB	■	Apache HTTP ■
Tomcat	■	Floating License ■
Performance Monitoring	■	SNMP Agent ■
PORTS STATUS		
HTTP	80	OPEN
IPP Files	8080	OPEN
IPP HTTP	8081	OPEN
IPP HTTPS	8082	OPEN
SEM HTTP	5000	OPEN
SEM HTTPS	5001	OPEN
HTTPS	443	OPEN

The Server Info page (**System > Administration > OVOC Server > Info**) presents information about the OVOC server including hardware info, components versions, NTP info, security info and network info. The feature saves operators from having to log in to the EMS Server Manager. The same information is presented only in friendlier format.

**Figure 3-6: Server Info page**

**SERVER INFO** Refresh

**ADMINISTRATION** <<

- LICENSE
  - Configuration
  - Tenants Allocations
  - Floating License
- SECURITY
  - Authentication
  - Operators
- OVOC SERVER**
  - Status
  - Info**
  - Configuration

**HARDWARE INFO**

Environment	Virtual
Server Type	VMware Virtual Platform
Spec	VM Entry Level Spec
CPU	Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz , cpu cores: 2 , total cpu:2
Memory Size	15885 MB
Swap Size	7.8 GB
Disk Size	536.9 GB

**COMPONENTS VERSIONS**

OVOC	7.6.1083
OS Revision	CentOS 7 for EM5 Server (Rev. 18)
OS Version	Linux 3.10.0-957.1.3.el7.x86_64 x86_64
Java	java full version "1.8.0_201-b09"
Cassandra DB	3.11.2
Apache	Server version: Apache/2.4.6 (CentOS) Server built: Nov 5 2018 01:47:09
Tomcat	8.5.32.0
NTP	ntpd 4.2.6p5

**NTP INFO**

NTP Client	Yes
Sync IP	+10.1.1.10
NTP Server	No
Date	Thu Feb 21 14:40:51 IST 2019

**SECURITY INFO**

File Integrity Checker	DOWN
IP Manager Protocol	HTTP
HTTPS Authentication	Mutual
QoE Client Protocol	HTTPS
QoE Devices Protocol	TCP

**NETWORK INFO**

Hostname	aclovoc01
IP Address	10.1.8.24
Interface Name	ens160
Subnet Mask	255.255.0.0
Network Address	10.1.0.0
Default Gateway	10.1.0.1

See [Securing Connections with FQDN or IP Address](#) below for information about the Server Configuration page (**System > Administration > OVOC Server > Configuration**).

## Securing Connections with FQDN or IP Address

Operators can optionally secure SSL connections with an IP address (default) or with an FQDN hostname.

Supported connections are:

- Device - OVOC server
- OVOC - LDAP Active Directory

### ➤ To implement the feature:

1. Open the Server Configuration page (**System > Administration > OVOC Server > Configuration**).

**Figure 3-7: Server Configuration**

**SERVER CONFIGURATION**

**ADMINISTRATION** <<

- LICENSE
  - Configuration
  - Tenants Allocations
  - Floating License
- SECURITY
  - Authentication
  - Operators
- OVOC SERVER**
  - Status
  - Info
  - Configuration**

**GENERAL SETTINGS**

OVOC Hostname: OVOC149

SBC Devices Communication: IP Based

Submit

2. From the 'SBC Devices Communication' drop-down list, select either **IP Based** (default) or **Hostname Based**.

## Customizing Call Storage

The OVOC's Server Call Storage page allows operators whose security level is configured as 'System' to customize the storage of calls on the OVOC server according to successful calls and/or failed calls (call performance) and the quality of the calls (good, fair/poor and/or unknown) in these two categories.

Operators can furthermore customize whether to include or exclude call flow and/or call trend.

### ➤ To customize call storage:

1. Open the Calls Storage page (**System > Administration > OVOC Server > Calls Storage**).

**Figure 3-8: Calls Storage**

CALLS STORAGE SETTINGS			
Calls Storage level: Custom			
<b>Successful Calls</b>			
	Save Calls	Include Call Flow	Include Call Trend
Good Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fair / Poor Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unknown Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<b>Failed Calls</b>			
	Save Calls	Include Call Flow	Include Call Trend
Good Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fair / Poor Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unknown Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

2. From the 'Calls Storage Level' drop-down, select either:
  - **Custom** (default) (see the figure above for the configured settings)
  - **Minimal** (see the following figure for the configured settings)
  - **Maximal** (all settings are selected)
  - **Recommended** (see the figure after the following for the configured settings)

**Figure 3-9: Calls Storage Level - Minimal**

Calls Storage level: **Minimal**

**Successful Calls**

	Save Calls	Include Call Flow	Include Call Trend
Good Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fair / Poor Quality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unknown Quality	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

---

**Failed Calls**

	Save Calls	Include Call Flow	Include Call Trend
Good Quality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fair / Poor Quality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Unknown Quality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Figure 3-10: Calls Storage Level - Recommended**

Calls Storage level: **Recommended**

**Successful Calls**

	Save Calls	Include Call Flow	Include Call Trend
Good Quality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fair / Poor Quality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Unknown Quality	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

---

**Failed Calls**

	Save Calls	Include Call Flow	Include Call Trend
Good Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fair / Poor Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Unknown Quality	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

3. Use the matrices below as reference.

**Table 3-2: Custom**

Call Performance	Call Quality	Save	Include Call Flow	Include Quality Trend
Success	Good	Yes	No	No
Success	Not Good (fair/poor)	Yes	No	Yes
Success	Gray	Yes	No	No

Call Performance	Call Quality	Save	Include Call Flow	Include Quality Trend
Fail	Good	Yes	Yes	No
Fail	Not Good (fair/poor)	Yes	Yes	Yes
Fail	Gray	Yes	Yes	No

**Table 3-3: Minimal**

Call Performance	Call Quality	Save	Include Call Flow	Include Quality Trend
Success	Good	No	No	No
Success	Not Good (fair/poor)	Yes	No	No
Success	Gray	No	No	No
Fail	Good	Yes	No	No
Fail	Not Good (fair/poor)	Yes	No	No
Fail	Gray	Yes	No	No

**Table 3-4: Recommended**

Call Performance	Call Quality	Save	Include Call Flow	Include Quality Trend
Success	Good	Yes	No	No
Success	Not Good (fair/poor)	Yes	No	Yes
Success	Gray	Yes	No	No
Fail	Good	Yes	Yes	No
Fail	Not Good (fair/poor)	Yes	Yes	Yes
Fail	Gray	Yes	Yes	No

**Table 3-5: Maximal**

Call Performance	Call Quality	Save	Include Call Flow	Include Quality Trend
Success	Good	Yes	Yes	Yes
Success	Not Good (fair/poor)	Yes	Yes	Yes
Success	Gray	Yes	Yes	Yes
Fail	Good	Yes	Yes	Yes
Fail	Not Good (fair/poor)	Yes	Yes	Yes
Fail	Gray	Yes	Yes	Yes



- If **Custom** is selected but settings are changed, the changed configuration is preserved and displayed during the next login.
- A change to call storage settings does not impact calls already saved on the OVOC server.
- All calls previously stored on the OVOC server are stored according to the previously configured settings and cleared using regular call clearing policy (time or size based).

See [Customizing Maximum Storage Period](#) on the next page

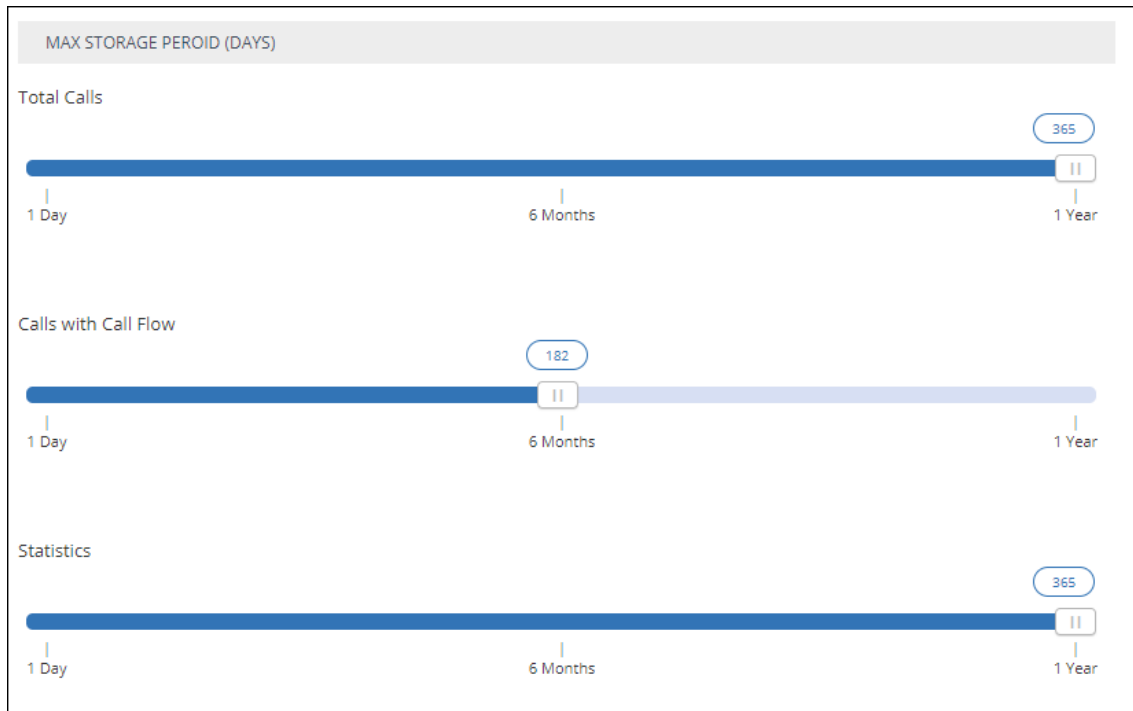
## Customizing Maximum Storage Period

The OVOC's Server Call Storage page allows operators whose security level is configured as 'System' to customize the maximum number of days call-related information will be stored on the OVOC server before it is cleared.

➤ **To customize the maximum storage period:**

1. Open the Calls Storage page (**System > Administration > OVOC Server > Calls Storage**) and locate the 'Max Storage Period (Days)' section of the page.

**Figure 3-11: Max Storage Period (Days)**



- Calls are checked daily and cleared from the OVOC server based on the values you configure.
- Default: 365 days (the maximum number of days call-related information can be stored on the OVOC server before it's cleared)
- Range: 1 day - 365 days

2. Drag and drop the 'Total Calls' slider to the maximum number of days you require *all calls* to be stored on the OVOC server before they're cleared.
3. Drag and drop the 'Calls with Call Flow' slider to the maximum number of days you require *calls together with call flow* to be stored on the OVOC server before they're cleared.
4. Drag and drop the 'Statistics' slider to the maximum number of days you require *call statistics* to be stored on the OVOC server before they're cleared.



If you configure the maximum number of days to a value lower than that which was previously configured (by another operator, say), *all data* will be cleared the next clearing.

## Configuration tab

The 'Configuration' tab lets you:

- configure global system templates (see [Configuring Templates](#) below)
- configure alarms settings (see [Configuring Alarms Settings](#) on page 69)
- add software and auxiliary files (see [Adding Configuration Files to the OVOC's Software Manager](#) on page 72)
- open external applications (see [Connecting Directly to External Applications](#) on page 76)
- back up (see [Backing up a Device's Configuration using Backup Manager](#) on page 112)

## Configuring Templates

The Templates folder allows you to configure the following global, system-wide templates to facilitate more effective network management:

- SNMP Connectivity (see [SNMP Connectivity](#) below)
- HTTP Connectivity (see [HTTP Connectivity](#) on page 65)
- QoE Thresholds (see [QoE Thresholds](#) on page 65)
- QoE Status & Alarms (see [QoE Status and Alarms](#) on page 67)
- Performance Monitoring Template (see [Adding a PM Template](#) on page 189)

## SNMP Connectivity

This template lets you configure an SNMP connectivity template whose parameter values can then be applied system-wide (globally). The template facilitates more effective network management. SNMP/HTTP templates are the default profile values for each defined tenant. The tenant SNMP/HTTP profiles are used as default for the devices under them.

### ➤ To configure an SNMP Connectivity template:

1. Open the SNMP Connectivity screen (**System > Configuration > Templates > SNMP Connectivity**).

**Figure 3-12: SNMP Connectivity Template**

2. Use the following table as a reference to the parameters in the figure above.

**Table 3-6: SNMP Connectivity Template**

Parameter	Description
<b>SNMP v2</b>	
SNMP Read Community	Enter an encrypted SNMP read community string. The default value for the SNMP read community string is 'public'.
SNMP Write Community	Enter an encrypted SNMP write community string. The default value for the SNMP write community string is 'private'.
SNMP Trap Community	Enter the Trap Community string to be received as part of the Notification message.
<b>SNMP v3</b>	
Security Name	Enter a name for SNMP v3. Example: OVOC User.
Security Level	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>Authentication and Privacy</b> (default)</li> <li>■ <b>No Security</b></li> <li>■ <b>Authentication</b></li> </ul>
Authentication Protocol	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>SHA</b> (default)</li> <li>■ <b>MDS</b></li> <li>■ <b>No Protocol</b></li> </ul>
Authentication Key	Enter an Authentication Key. Default: 123456789.
Privacy Protocol	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>AES 128</b> (default)</li> <li>■ <b>DES</b></li> </ul>
Privacy Key	Enter a Privacy Key. Default: 123456789.

3. Click **Submit**.

## HTTP Connectivity

This option lets you configure an HTTP connectivity template whose parameter values can then be applied system-wide (globally) when adding multiple AudioCodes devices, for example. The template facilitates more effective network management for OVOC operators.

➤ **To configure an HTTP Connectivity template:**

1. Open the HTTP Connectivity screen (**System > Configuration > Templates > HTTP Connectivity**).

**Figure 3-13: HTTP Connectivity Template**

2. Use the following table as a reference to the parameters in the preceding figure.

**Table 3-7: HTTP Connectivity Template**

Parameter	Description
Device Admin User	Enter the device Web server user name. Example: <b>Admin</b> . Password - "Admin".
Device Admin Password	Enter the Web server password. Example: <b>Admin</b> .
Default Connectivity	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>HTTP</b> (default)</li> <li>■ <b>HTTPS</b></li> </ul>

3. Click **Submit**.

## QoE Thresholds

QoE Thresholds determine *global* (system-wide) voice quality thresholds templates.

[For information on how to configure QoE Thresholds profiles *per tenant*, see [Managing QoE Thresholds Profiles per Tenant](#) on page 252]

Three QoE Thresholds templates (Low | Medium | High Sensitivity) for the voice quality metrics of MOS, Delay, Packet Loss, Echo and Jitter are accessed in the page. In the page, you can add, edit or delete a voice quality thresholds template.

➤ To access the global QoE thresholds templates:

1. From the System menu, open the QoE Thresholds page (**System > Configuration > Templates > QoE Thresholds**).

**Figure 3-14: QoE Thresholds Templates**

QOE THRESHOLDS		NAME	DESCRIPTION	MOS	DELAY (MSEC)	PLOSS (R)	JITTER (MSEC)	ECHO (DB)
CONFIGURATION	TEMPLATES	Medium Sensitivity Th...		→ 3.5 → → 2.8 →	→ 160 → → 500 →	→ 2 → → 5 →	→ 40 → → 80 →	→ 30 → → 10 →
		High Sensitivity Thres...		→ 3.4 → → 2.9 →	→ 140 → → 400 →	→ 1.5 → → 4.3 →	→ 35 → → 70 →	→ 27 → → 11 →
		Low Sensitivity Thresh...		→ 3.4 → → 2.6 →	→ 200 → → 1,200 →	→ 2.7 → → 6.6 →	→ 45 → → 90 →	→ 23 → → 9 →

QOE THRESHOLD DETAILS	
NAME	High Sensitivity Threshold
DESCRIPTION	
MOS	→ 3.4 → → 2.9 →
DELAY (MSEC)	→ 140 → → 400 →
PLOSS (R)	→ 1.5 → → 4.3 →
JITTER (MSEC)	→ 35 → → 70 →
ECHO (DB)	→ 27 → → 11 →

In the page, you can see three *global* (system-wide) QoE thresholds templates displayed. Each consists of threshold values set for the voice quality metrics of MOS, Delay, Packet Loss, Echo and Jitter, for each call quality category of 'Poor', 'Fair' and 'Good'. Use the following table as reference to the figure above.

**Table 3-8: QoE Thresholds Templates**

Template	Description
Low Sensitivity Threshold	Threshold values representing recommended data for the 'Low' sensitivity level.
Medium Sensitivity Threshold	Threshold values representing recommended data for the 'Medium' sensitivity level.
High Sensitivity Threshold	Threshold values representing recommended data for the 'High' sensitivity level.

2. Select a template and then click **Edit**.

**Figure 3-15: QoE Thresholds Settings**

**QOE THRESHOLDS DETAILS**

Threshold Name \*

Description

Defaults: All | None | Invert

☒ Device ☒ Link ☒ Endpoint

---

THRESHOLD VALUES

**Status Threshold Values**

<input checked="" type="checkbox"/> MOS (0-5)	<input type="text" value="3.5"/>	<input type="text" value="3"/>
<input checked="" type="checkbox"/> Delay (Msec)	<input type="text" value="160"/>	<input type="text" value="500"/>
<input checked="" type="checkbox"/> PLoss (%)	<input type="text" value="2"/>	<input type="text" value="5"/>
<input checked="" type="checkbox"/> Jitter (Msec)	<input type="text" value="40"/>	<input type="text" value="80"/>
<input checked="" type="checkbox"/> Echo (DB)	<input type="text" value="25"/>	<input type="text" value="10"/>

OK Close

3. Provide an intuitive name for the profile. As a reference, use the names of the three QoE Threshold Templates displayed in the table above.
4. Enter a description of the profile to facilitate effective intuitive management later.
5. Select the **Device** option to set the profile as devices default.
6. Select the **Links** option to set the profile as links default.
7. Select the **Endpoints** option to set the profile as endpoints default.
8. By default, **All** metrics are included in the profile. To *exclude* a metric, clear its check box. To define the MOS metric, for example, click the bar or drag the markers. Each bar unit increments or decreases the threshold by **0.1 (MOS, Packet Loss)**, or by **1 (Delay, Jitter, Echo)**.
9. Do the same for the other metrics thresholds.
10. Click **OK**; the profile is displayed in the QoE Thresholds screen.

## QoE Status and Alarms

The QoE Status and Alarms page determines the *global (system-wide)* QoE status of devices, sites, links and endpoints. The page provides a centralized view of global QoE alarms and statuses. For information on managing QoE Status *per tenant*, see [Managing QoE Status and Alarms per Tenant](#) on page 258.

## ➤ To view the global QoE status:













1. From under the System menu, open the QoE Status and Alarms page (**System > Configuration > Templates > QoE Status & Alarms**).




Figure 3-16: QoE Status and Alarms

QOE STATUS & ALARMS											
CONFIGURATION <<		DEFAULTS	NAME	LAST RUNTIME	MONITORING FREQU...	MINIMUM CALLS PER...	FAILED CALLS PROFILE (%)	POOR QUALITY CALLS RULE (%)	AVERAGE CALL DURATION RUL...	BANDWIDTH RULE (KB/SEC)	MAX CONCURRENT CALLS RUL...
# TEMPLATES SIP/MP Connectivity HTTP Connectivity QoE Thresholds <b>QoE Status &amp; Alarms</b> ALARMS FILE MANAGER EXTERNAL APPLICATIONS DEVICE BACKUP			ALARM RULE		15	50	+2+ +10+	+2+ +10+	+3+ +3+	+10+ +1+	+10+ +1+

2. Use the following table as reference to the figure above.

Table 3-9: QoE Status and Alarms

Page Indications	Description
Defaults	 = displayed when the alarm rule applies to devices  = displayed when the alarm rule applies to links  = displayed when the alarm rule applies to sites  = displayed when the alarm rule applies to IP phones
Name	Indicates the name of the alarm rule.
Last Runtime	Indicates the last time the alarm rule was activated.
Monitoring Frequency Min	Indicates at least how often monitoring is performed. Default: 15
Minimum Calls per Entity to Analyze	Indicates the minimum number of calls to analyze, per entity. Default: 50
Failed Calls (%)	<p>  <b>x</b>  <b>y</b>  indicates that green changes to orange ('Major' severity) when the <b>x</b> percentage of failed calls is exceeded and orange changes to red ('Critical' severity) when the <b>y</b> percentage of failed calls is exceeded.           </p> <p>  indicates alarm issued – displayed if the <b>Generate Alarm</b> option is selected in the Alarm Rule Details screen (see <a href="#">Adding a QoE Alarm Rule per Tenant</a> on page 258).           </p>
Poor Quality Calls (%)	<p>  <b>x</b>  <b>y</b>  indicates that green changes to orange ('Major' severity) when the <b>x</b> percentage of poor quality calls is exceeded and orange changes to red ('Critical' severity) when the <b>y</b> percentage of of poor quality calls is exceeded.           </p> <p>  indicates alarm issued – displayed if the <b>Generate Alarm</b> option is selected in the Alarm Rule Details screen (see <a href="#">Adding a QoE Alarm Rule per Tenant</a> on page 258).           </p>

Page Indications	Description
Average Call Duration (seconds)	<p>➔ <b>x</b> ➔ <b>y</b> ➔ indicates that green changes to orange ('Major' severity) when <b>x</b> seconds call duration is exceeded and orange changes to red ('Critical' severity) when <b>y</b> seconds call duration is exceeded.</p> <p> indicates alarm issued – displayed if the <b>Generate Alarm</b> option is selected in the Alarm Rule Details screen (see <a href="#">Adding a QoE Alarm Rule per Tenant</a> on page 258).</p>
Bandwidth Rule (Kbps)	<p>➔ <b>x</b> ➔ <b>y</b> ➔ indicates that green changes to orange ('Major' severity) when <b>x</b> bandwidth is exceeded and orange changes to red ('Critical' severity) when <b>y</b> bandwidth is exceeded.</p> <p> indicates alarm issued – displayed if the <b>Generate Alarm</b> option is selected in the Alarm Rule Details screen (see <a href="#">Adding a QoE Alarm Rule per Tenant</a> on page 258).</p>
Maximum Concurrent Calls (#)	<p>➔ <b>x</b> ➔ <b>y</b> ➔ indicates that green changes to orange ('Major' severity) when <b>x</b> concurrent calls is exceeded and orange changes to red ('Critical' severity) when <b>y</b> concurrent calls is exceeded.</p> <p> indicates alarm issued – displayed if the <b>Generate Alarm</b> option is selected in the Alarm Rule Details screen (see <a href="#">Adding a QoE Alarm Rule per Tenant</a> on page 258).</p>

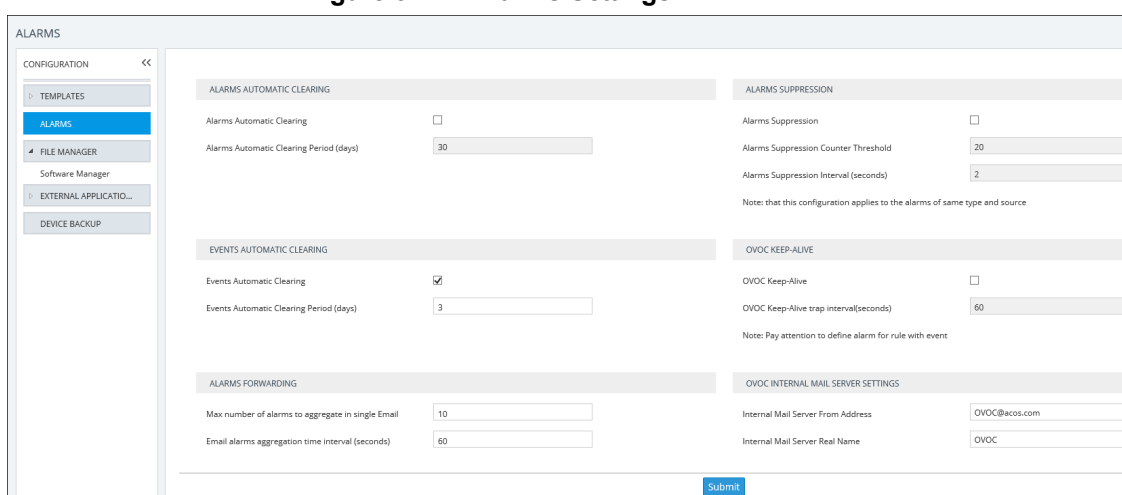
## Configuring Alarms Settings

The Alarms screen allows you to configure how alarms and events are displayed in the Alarms pages.

### ➤ To configure alarm settings:

1. Open the Alarms page (**System > Configuration > Alarms**).

**Figure 3-17: Alarms Settings**



**ALARMS**

**CONFIGURATION** <<

- TEMPLATES
- ALARMS**
- FILE MANAGER
  - Software Manager
- EXTERNAL APPLICATIONS
- DEVICE BACKUP

**ALARMS AUTOMATIC CLEARING**

Alarms Automatic Clearing ☐

Alarms Automatic Clearing Period (days)

**EVENTS AUTOMATIC CLEARING**

Events Automatic Clearing ☒

Events Automatic Clearing Period (days)

**ALARMS SUPPRESSION**

Alarms Suppression ☐

Alarms Suppression Counter Threshold

Alarms Suppression Interval (seconds)

Note: that this configuration applies to the alarms of same type and source

**OVOC KEEP-ALIVE**

OVOC Keep-Alive ☐

OVOC Keep-Alive trap interval(seconds)

Note: Pay attention to define alarm for rule with event

**ALARMS FORWARDING**

Max number of alarms to aggregate in single Email

Email alarms aggregation time interval (seconds)

**OVOC INTERNAL MAIL SERVER SETTINGS**

Internal Mail Server From Address

Internal Mail Server Real Name

**Submit**

2. Configure the alarms settings using the following table as reference.

**Table 3-10: Alarms Settings**

Setting	Description
Alarms Automatic Clearing	<p>Select this option to clear all devices listed in the Alarms page of all active alarms when the system starts up (cold start event): Critical, Major, Minor, Warning or Info.</p> <p>Use this setting to prevent historical, dated alarms from cluttering the Alarms page.</p>
Alarms Automatic Clearing Period (Days)	<p>[Only relevant if the 'Alarms Automatic Clearing' option is selected]</p> <p>Clears old alarms after a defined period of days even though a Clear alarm to stop displaying very old active alarms has not been received from the device.</p>
Events Automatic Clearing	<p>Select this option for device events (events originating from the device) to be automatically cleared from the Alarms page when the system starts up (cold start event).</p> <p>Device events originating in the OVOC, e.g., adding a gateway, are not cleared when the device is reset. The OVOC consequently employs a mechanism to automatically clear these events from the Alarms page. The feature prevents historical, dated events from cluttering the Alarms page.</p>
Events Automatic Clearing Period (days)	<p>Events are by default cleared every three days. You can change the default to suit your requirements.</p>
Max number of alarms to aggregate in single Email	<p>If an alarms forwarding rule is configured (under Alarms &gt; Forwarding), the alarms can be aggregated to be sent in a single email. This parameter allows you to configure the maximum number of alarms to aggregate in a single email. Default: 10. If, for example, the number of alarms to aggregate is configured to 10 and the time interval (see the next parameter) is configured to 60 seconds, then after 60 seconds, five alarms will be raised according to the alarms forwarding rule and five aggregated alarms will be forwarded.</p>
Email alarms aggregation time interval (seconds)	<p>If an alarms forwarding rule is configured (under Alarms &gt; Forwarding) and the alarms are configured to be aggregated and sent in a single email, you can configure a time interval to determine how often aggregated alarms are forwarded. Default: 60. If, for example, the number of alarms to aggregate is configured to 10 (see the previous parameter) and the time interval is configured to 60 seconds, then after 60 seconds, five alarms will be raised according to the alarms forwarding rule and five aggregated alarms will be forwarded.</p>
Alarms Suppression	<p>Select this option for an 'Alarm Suppression' alarm to be generated when the OVOC server identifies that the number of alarms of the same type and from the same source, generated in a time period, is greater than the number defined in the threshold. At this point, these alarms are not added to the database and are not forwarded to configured destinations.</p>

Setting	Description
Alarms Suppression Counter Threshold	[Only applicable if 'Alarms Suppression' is selected] Lets you configure a counter threshold (Default: 10 alarms) and interval (Default: 10 seconds). For example, if 10 alarms are generated from 'Board#1/EthernetLink#2' in 10 seconds, then alarms from this source are suppressed and the 'Suppression' alarm is generated. This alarm is cleared if in the subsequent 10 second interval, less than 10 alarms are sent from this source. At this point, updating the OVOC database is resumed (the last received alarm is updated).
Alarms Suppression Interval (seconds)	During the time the suppression alarm is active, the OVOC server updates the database with a single alarm (with updated unique ID) database every minute, until the alarm is cleared.
OVOC Keep-Alive	Select this option for the OVOC to generate SNMP Keep-alive traps to 3rd-party applications, such as a Syslog server. This trap can be sent to either the SNMP, Syslog or Mail server destination. You can send the Keep-Alive trap to the target destination, according to an existing configured forwarding destination rule.
OVOC Keep-Alive trap interval (seconds)	[Only applicable if 'OVOC Keep-Alive' is selected] Determines how frequently the trap is sent from the OVOC to the configured destination. Default: Every 60 seconds. You can configure a different interval to suit your requirements.
Internal Mail Server From Address	<p>If your enterprise uses OVOC's internal email server for Alarms Forwarding, use this parameter to configure the internal mail server's 'From Address'.</p> <p>For example, if you configure <b>john.brown@enterprisename.com</b> for this parameter and you configure <b>John Brown</b> for the parameter following in this table ('Internal Mail Server Real Name'), then all alarms forwarded from OVOC by email from rules configured with 'Use Internal Mail Server' will be from address:</p> <p><b>john.brown@enterprisename.com &lt; John Brown &gt;</b></p> <p>See related parameters 'Forward matching alarms/events', 'Prevent forwarding matching alarms/events' and 'Enable/Disable Rule' under <a href="#">Forwarding Alarms</a> on page 167.</p>
Internal Mail Server Real Name	<p>If your enterprise uses OVOC's internal email server for Alarms Forwarding, use this parameter to configure the internal mail server's 'Real Name'.</p> <p>For example, if you configure <b>John Brown</b> for this parameter and you configure <b>john.brown@enterprisename.com</b> for the preceding parameter in this table ('Internal Mail Server From Address'), then all alarms forwarded from OVOC by email from rules configured with 'Use Internal Mail Server' will be from address:</p> <p><b>john.brown@enterprisename.com &lt; John Brown &gt;</b></p> <p>See related parameters 'Forward matching alarms/events', 'Prevent forwarding matching alarms/events' and 'Enable/Disable Rule' under <a href="#">Forwarding Alarms</a> on page 167.</p>

## Adding Configuration Files to the OVOC's Software Manager

You can add ini files, cmp firmware files, cli files, conf files and auxiliary files to the OVOC's Software Manager in order to load them to devices.

The Software Manager page lets operators view, add or remove files. Filters facilitate quick and easy access to device-specific files.

After defining a device in the OVOC, the OVOC connects to it and automatically determines its version. Each *new* version, fix or software update provided to customers must be added to the Software Manager, to enable upgrading device software.

Files per network device include:

- SBC configuration files (ini, cli, conf)
- MSBR (cli)
- SBC software files (cmp)
- MP-202 software files (rms/rmt)
- IP phone firmware files
- IP phone configuration files (templates)
- MP-202 configuration files (conf)
- Auxiliary files (prt, cpt, etc.)

Use the following table as a reference with respect to which operator type is permitted to perform what file management.

**Table 3-11: OVOC Software File Management per Operator Type**

Operator Type	Permitted to Perform this File Management
System (except operators with 'Monitoring' security level)	<ul style="list-style-type: none"> <li>■ Add any global file that will not be assigned to any specific tenant. These files will be visible to both 'tenant' and 'system' operator types.</li> <li>■ Add a file and assign it to a specific tenant. These files will be visible to both 'tenant' and 'system' operator types.</li> <li>■ Download any file visible by the tenant (Added by 'tenant' and 'system' operator types) to any device in the tenant.</li> <li>■ Remove any file added by 'tenant' and 'system' operator types.</li> </ul>
Tenant (except operators with 'Monitoring' security level)	<ul style="list-style-type: none"> <li>■ Add any file. This file will be assigned only to the tenant. These files will be visible to both 'tenant' and 'system' operator types.</li> <li>■ Download any file visible by the tenant to the devices in the tenant.</li> <li>■ Remove any file added by a 'tenant' operator type.</li> </ul>



- Only one SBC software file (cmp) with the same version for a specific product type can be added to a tenant.
- Software files cannot be shared between tenants (except global). If an operator assigned to multiple tenants adds a file, it can be downloaded only on devices in a specific tenant and not to all tenants.

## Adding the ini File

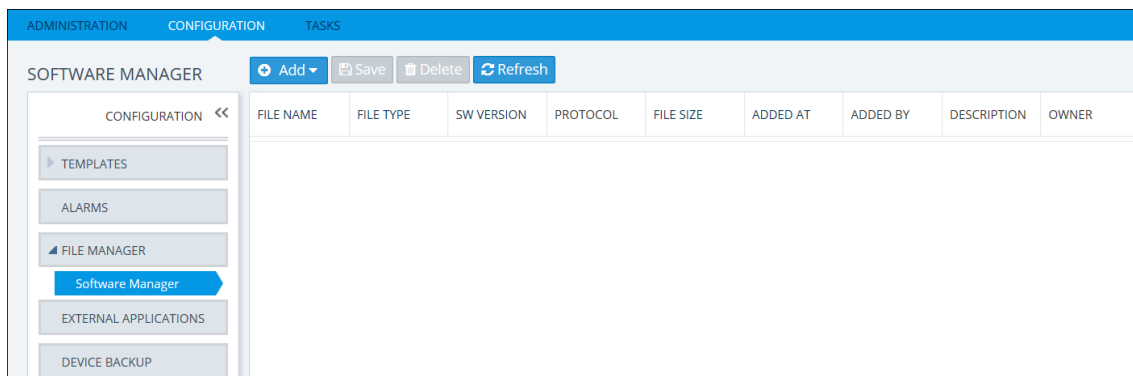
You can add the ini file to the OVOC's Software Manager in order to perform initial configuration of device parameters which cannot be configured after defining the device in the OVOC. When loading the ini file to the device, operators can choose either:

- Full Configuration ini file download – with validation and apply (recommended)
- Full Configuration ini file download – without validation and apply (for software upgrade)
- Incremental ini file download (the previous configuration remains)

### ➤ To add the ini file to the OVOC:

1. Open the Software Manager page (**System > Configuration > File Manager > Software Manager**).

**Figure 3-18: Software Manager**



2. Click **Add** and select **Add Auxiliary File** from the menu drop-down.

**Figure 3-19: Add Auxiliary File – ini File**

3. From the 'Tenant' drop-down, select the tenant under which the ini file will be added.
4. From the 'File Type' drop-down, select **INI** (default) if it isn't selected already.

5. Next to the 'File Name' field, click the folder icon and browse to the ini file's location.
6. Enter a description of the file in the 'File Description' pane for intuitive future file management, and then click **OK**; the ini file is added to the Software Manager.

### Adding a cmp File

You can add a firmware (cmp) file to the OVOC to later load to the device. With the exception of the MP-20x media gateways, the cmp files are the devices' main software firmware image files. You can add a cmp file to the OVOC in order (for example) to change the software version.

➤ **To add a cmp file to the OVOC:**

1. Open the OVOC's Software Manager page (**System > Configuration > File Manager > Software Manager**).
2. Click **Add** and select **Add Software File** from the drop-down menu.

**Figure 3-20: Add Software File**

3. From the 'Tenant' drop-down, select the tenant under which the cmp file will be added.
4. Next to the 'CMP' field, click ... and browse to the cmp file's location.
5. Enter a description of the file in the 'File Description' pane for intuitive future file management.
6. In the 'Software Version' field, enter the version of the software file. If left undefined, the field will be automatically defined after adding the cmp or rmt/rms file.
7. From the 'Major Version' drop-down, select the device version (Default: 6.6).
8. From the 'Select Product' drop-down list, select the relevant product corresponding to the cmp or rmt/rms file.
9. From the 'Select Protocol' drop-down, select the protocol. Default: SIP. MGCP and MEGACO are also available.

10. Click **OK**; the cmp file is added to the Software Manager.

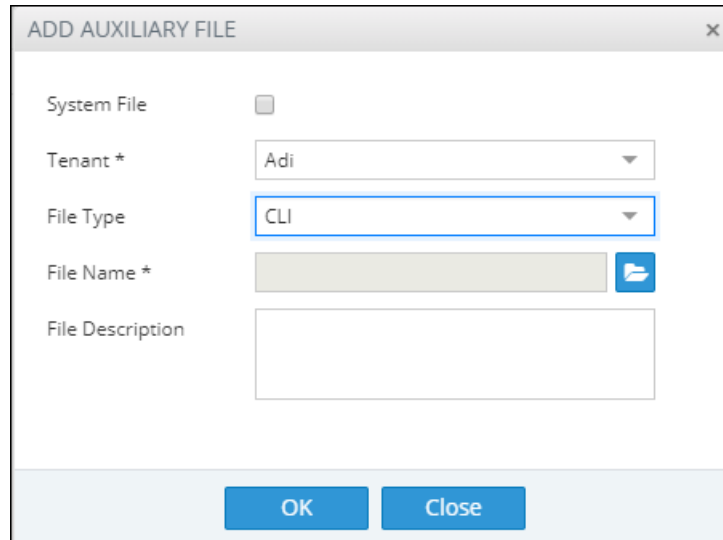
## Adding a cli File

A cli file can be added to the OVOC to later load to the MSBR devices and SBC Linux devices.

### ➤ To add a cli file to the OVOC:

1. Open the OVOC's Software Manager page (**System > Configuration > File Manager > SoftwareManager**).
2. Click **Add** and select **Add Auxiliary File** from the drop-down menu.

**Figure 3-21: Add Auxiliary File**



The screenshot shows a dialog box titled "ADD AUXILIARY FILE". It contains the following fields and controls:

- System File**: A checkbox that is currently unchecked.
- Tenant \***: A dropdown menu with "Adi" selected.
- File Type**: A dropdown menu with "CLI" selected.
- File Name \***: A text input field with a file browser icon to its right.
- File Description**: A larger text input area.
- Buttons**: "OK" and "Close" buttons at the bottom.

3. From the 'Tenant' drop-down, select the tenant under which the cli file will be added.
4. From the 'File Type' drop-down, select CLI.
5. Next to the 'File Name' field, click the browser icon to browse to the cli file's location.
6. Enter a description of the file in the 'File Description' pane for intuitive future file management.
7. Click **OK**; the cli file is added to the Software Manager.

## Adding Auxiliary Files

Besides the ini file, you can add auxiliary files to the OVOC's Software Manager.

### ➤ To add an auxiliary file to the OVOC's Software Manager:

1. Open the OVOC's Software Manager page (**System > Configuration > File Manager > Software Manager**).
2. Click **Add** and select **Add Auxiliary File** from the drop-down menu.
3. From the 'Tenant' drop-down, select the tenant under which to add the auxiliary file.
4. From the 'File Type' drop-down list, select the auxiliary file to be added.

**Figure 3-22: Add Auxiliary File**



- See the device's *User's Manual* for more information about device-related files.
- The CERTIFICATE file secures the following connections:
  - ✓ Active Directory server (domain controller)
  - ✓ MSSQL Front End server
  - ✓ LDAP User Authentication
- The X.509 PRIVATE KEY, X.509 CERTIFICATE and X.509 TRUSTED ROOT CERTIFICATE files are AudioCodes certificate files that secure the connection between OVOC and the devices.
  - ✓ The X.509 files are for all the security files, including LDAP.
- These files may be default AudioCodes certificate files or files generated by an external CA. For more information about certification implementation, see the *One Voice Operations Center Security Guidelines*.

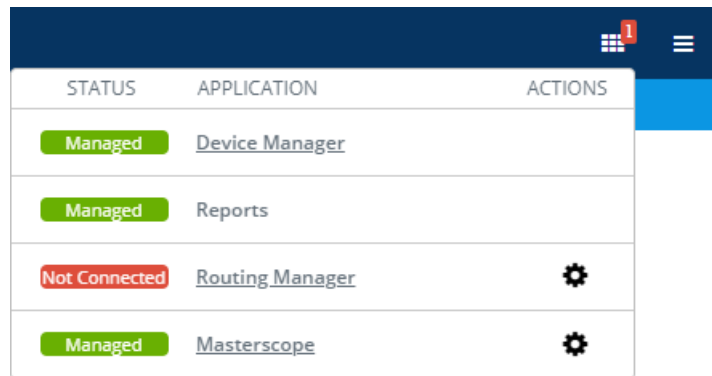
5. Enter a description of the file in the 'File Description' pane for intuitive future file management.
6. Next to the 'File Name' field, click ... and browse to the file's location.
7. Enter a description of the file in the 'File Description' pane for intuitive future file management, and then click **OK**; the file is added to the Software Manager.

## Connecting Directly to External Applications

The OVOC features an external applications menu that allows operators to directly connect to IP telephony network management applications, both of AudioCodes as well as of external vendors. These applications enable comprehensive control over any enterprise or ITSP IP telephony network, helping providers deliver the quality of service users require.

### ➤ To directly access the external applications menu:

1. On every page of the OVOC on the right of the title bar, click the  icon.



STATUS	APPLICATION	ACTIONS
Managed	<a href="#">Device Manager</a>	
Managed	<a href="#">Reports</a>	
Not Connected	<a href="#">Routing Manager</a>	⚙️
Managed	<a href="#">Masterscope</a>	⚙️

- Click the relevant link for single sign-on to:
  - ◆ [Device Manager](#) (see [Device Manager](#) below for more information)
  - ◆ [Reports](#) (see for [Reports](#) below more information)
  - ◆ [Routing Manager](#) (see [ARM](#) on the next page for more information)
  - ◆ [MasterScope](#) (see [MasterScope](#) on page 79 for more information)

## Device Manager

The external applications menu allows operators to directly access the Device Manager, a life cycle management application for enterprise IP phone deployments that enables administrators to deliver a reliable desktop phone service within their organization. With the ability to deploy and monitor IP telephony devices, identify problems, and then fix them rapidly and efficiently, the application enhances employee satisfaction, increases productivity and lowers IT expenses.

### ➤ To directly access the Device Manager:

1. Click the applications menu icon located on every OVOC GUI page on the right of the title bar, and then click the **Device Manager** link.



- If your browser is configured to block pop-ups, a message will appear indicating 'Pop-ups were blocked on this page' (or similar). In this case, set your browser to allow pop-ups.
- The status of the application as well as the statuses of other applications can be viewed in the menu. The example in the figure above indicates that the network is managed by Device Manager and that there are no alarms in the network managed by Device Manager since the link is color-coded green.

2. View the Device Manager application which opens in a new browser tab.

## Reports

The external applications menu allows operators to directly access reports-generation capability that operators can utilize to distribute session experience data and comparative analysis to responsible persons within the enterprise and to external authorities associated with the enterprise's IP telephony network, for accurate diagnosis and correction of degraded sessions and for general network optimization.

### ➤ To directly access the reports-generation application:

1. In the applications menu located on every page on the right of the title bar, click the **Reports** link.



- If your browser is configured to block pop-ups, a message will appear indicating 'Pop-ups were blocked on this page' (or similar). In this case, set your browser to allow pop-ups.
- The status of the application as well as the statuses of other applications can be viewed in the menu. The example in the figure above indicates that the network is managed by AudioCodes Reports and that there are no alarms in the network managed by the application since the link is color-coded green.

2. View the reports-generation application which opens in a new browser tab. See [Producing Reports](#) on page 271 for more information.

## ARM

The external applications menu lets operators directly access the Routing Manager (ARM) for managing the dial plan and call routing rules of multi-site, multi-vendor enterprise VoIP networks. The ARM enables centralized control of all session routing decisions. Through the ARM's graphical user interface, network administrators can design and modify their voice network topologies and call routing policies from a single location, resulting in significant time and cost savings. Time-consuming tasks such as adding a new PSTN or SIP trunk interconnection, adding a new branch office or modifying individual users' calling privileges can be carried out simply and rapidly.

### ➤ To enable a direct connection to the ARM:

1. Open the External Applications page (**System > Configuration > External Applications**) as shown in the following figure, and then click the **ARM** option.

**Figure 3-23: External Applications - ARM**

2. In the field 'ARM Server FQDN / IP' under the General section, enter the FQDN (host name) or IP address of the ARM server to connect to. You can obtain these from your enterprise's network administrator if necessary.
3. Note that parameters 'ARM Status', 'ARM Version' and 'Unique Identifier' are *provisional placeholders*. They will be automatically reconfigured with true values after connection with the ARM is established.
4. Under the OVOC-ARM Communication section, you can select the Secure Communication option for HTTPS secured communications between OVOC-ARM.
5. Under the same section, if an OVOC-ARM connection has already been established, you can opt to configure the 'Change ARM Password' parameter value.

6. Under the ARM Single Sign On section, you can optionally configure direct sign-on to the ARM. Admin *and* Operator types can configure this SSO connection. Note that the feature applies only to ARM versions that support it. The logic is identical to the logic of a regular sign on (see the previous two steps).
7. Under the ARM-OVOC Communication section, select an OVOC operator. This operator will then be defined in the ARM in order to use the ARM.
8. Click **Submit**.
9. In any OVOC page, click the external applications menu icon displayed on the right side of the title bar.



- If your browser is configured to block pop-ups, a message will appear indicating 'Pop-ups were blocked on this page' (or similar). In this case, set your browser to allow pop-ups.
- ARM status as well as the statuses of other applications can be viewed in the menu. The example in the preceding figure indicates that the network is not managed by the ARM (Not Connected) and that there is an alarm in the ARM-managed network whose severity is Critical. If the color code had been green, the indication would have been that the network is managed by the ARM and that there are no alarms in the ARM-managed network.

10. In the external applications menu that opens, click the **Routing Manager** link.
11. View if you configured SSO the ARM's main screen which opens in a new browser tab. If you didn't configure SSO, you'll be prompted to log in.

## MasterScope

The External Applications page enables connecting directly to MasterScope in order to quickly and easily access the exact network equipment component associated with a voice quality issue - if an issue is detected - and benefit from root cause analysis. In this page, operators configure the connection, a.k.a. Single Sign On (SSO), to MasterScope. A MasterScope link is then displayed on the Call Details page.



Applies only to operators who have acquired and installed MasterScope.

### ➤ To enable connecting directly to MasterScope:

1. Open the External Applications page (**System > Configuration > External Applications**) as shown in the figure below and then click the **MasterScope** option.

**Figure 3-24: MasterScope**

The screenshot shows the MasterScope configuration interface. On the left, a sidebar menu includes sections like CONFIGURATION, TEMPLATES, ALARMS, FILE MANAGER, EXTERNAL APPLICATIONS, and DEVICE BACKUP. Under EXTERNAL APPLICATIONS, the 'MasterScope' link is highlighted. The main content area, titled 'MASTERSCOPE SERVER CONFIGURATION', features a text input field for 'Master Scope URL \*' containing the text 'ARM.BS.LAB.QA-EMS.LOCAL' and a blue 'Submit' button.

2. In the 'MasterScope URL' field, enter the MasterScope IP address or FQDN. This is a string type parameter. Maximum size: 100 characters.
3. Click **Submit**; the **MasterScope** link for single sign-on is displayed in the applications menu located on every OVOC page on the right of the title bar.



- If your browser is configured to block pop-ups, a message will appear indicating 'Pop-ups were blocked on this page' (or similar). In this case, set your browser to allow pop-ups.
- MasterScope status as well as the statuses of other applications can be viewed in the menu. The example in the preceding figure indicates that the network is managed by MasterScope and that there are no alarms in the MasterScope-managed network since the link is color-coded green.

4. Click the **MasterScope** link; the application opens in a new browser tab.

## Enabling Automatic Device Backup Periodically

The OVOC can be configured to automatically (daily) back up device configurations (ini, conf or cli script files) according to the OVOC server application's time. The files are saved on the OVOC server. They can be accessed and transferred using SSH and SFTP. The backup files are managed by the Backup Manager.

### ➤ To configure automatic device configuration backup:

1. Open the Device Backup page (**System > Configuration > Device Backup**).

**Figure 3-25: Device Backup**

The screenshot shows the 'DEVICE BACKUP' configuration page. On the left, a sidebar lists navigation options: CONFIGURATION, TEMPLATES, ALARMS, FILE MANAGER (which is selected and expanded to show 'Software Manager' and 'EXTERNAL APPLICATIONS'), and a 'DEVICE BACKUP' button. The main panel, titled 'DEVICE BACKUP', contains the following settings:

- Enable Periodic backup:** A checkbox that is checked.
- Number of backup files per device:** A text input field containing the value '3'.
- Number of retries:** A text input field containing the value '4'.

A blue 'Submit' button is located at the bottom right of the main panel.

2. Select the 'Enable Periodic backup' option.
  - When enabled, backup is automatically performed daily; all device configuration files (ini, conf and cli) are backed up to the Backup Manager from all devices.
  - When disabled, you can perform manual backup after making changes to a device's configuration (see [Backing up a Device's Configuration using Backup Manager](#) on page 112 for information about manually backing up a device's configuration).
3. Configure 'Number of backup files per device' to determine the number of latest backup files to be stored for each managed device. Default: 5.
4. In the 'Number of retries' field, configure the number of retries to be made each connection attempt to the device. Default: 2.
5. Click **Submit**.

## Tasks tab

The Tasks page displays asynchronous actions performed by operators, currently under execution. Tasks that are *in progress* are displayed irrespective of how long it takes for them to complete. The OVOC continues to display them 20 minutes after they're completed. They are then removed from the page.



If the operator is not a 'system' operator, *only tasks performed by that operator* are displayed in the Tasks page.

## Displaying the Status of Tasks Currently Under Execution

Adding multiple AudioCodes devices to the OVOC can be configured. OVOC supports many types of asynchronous actions. Adding multiple devices, described here, is just one example. As you can see in the figure, the operator is adding 10 AudioCodes devices whose IP addresses range from 10.1.1.1 to 10.1.1.10, under the region US.

**Figure 3-26: Task - Add Multiple AudioCodes Devices**

**MULTIPLE AUDIO CODES DEVICES DETAILS**

**GENERAL**    **SNMP**    **HTTP**    **FIRST CONNECTION**

Name Prefix \*

Description

Tenant

Region \*

☒ Enter IP Address Range

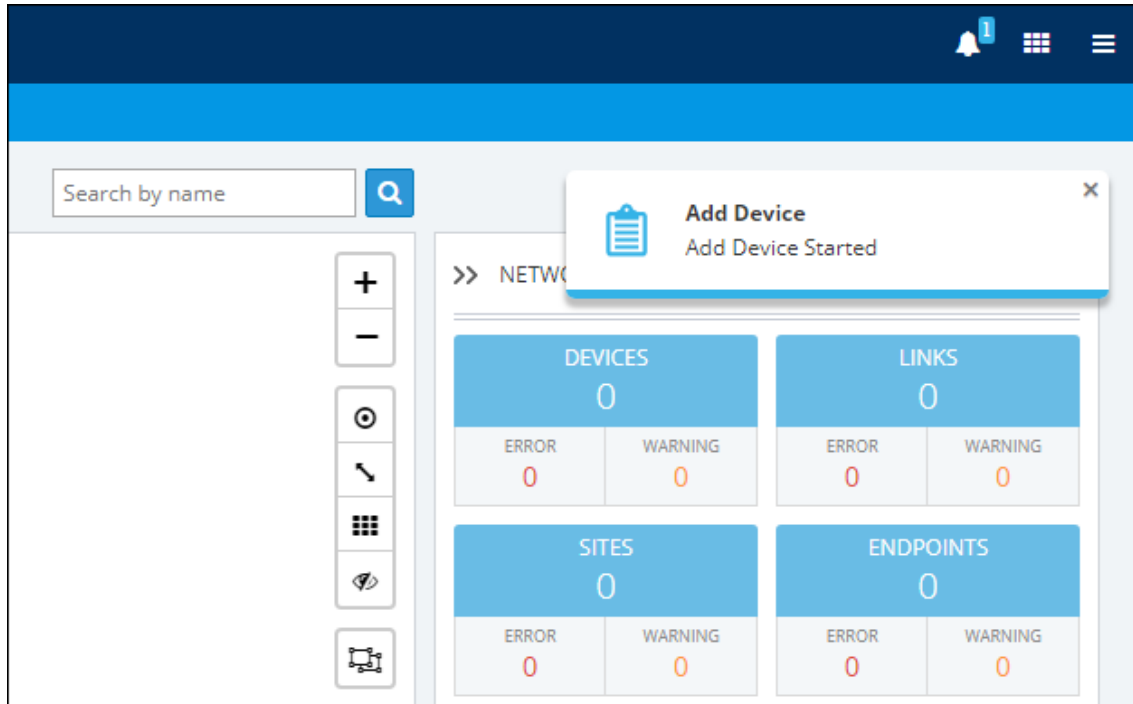
From \*

To \*

☐ Enter IP Address List

☐ Enter Serial Number List

- [Optional] In the 'Address' field, enter the first letters of the name of the city / country in which to locate the device, and then select the city / country from the list that pops up.
- After clicking **OK**, a notification pops up in the uppermost right corner indicating the task status.

**Figure 3-27: Example of a Notification Pop-up Indicating Task Status**

To configure the *timeout* of the notification pop-up, see [Configuring Operator Authentication Locally, in the OVOC](#) on page 34 and refer to the parameter 'Notifications display time (sec)'. The default is 3 seconds. Configuring the parameter to 0 disables the notification pop-up feature.

- Optionally, you can click a notification to open the Tasks page displaying the task about which you were notified.

**Figure 3-28: Tasks Page Showing Task Status - Adding Multiple AudioCodes Devices**

TASKS			
TASKS <<			
<div> <div> </div> <div> <b>ADD DEVICE</b>            10 entities   acladmin         </div> <div> <div></div> <div>100%</div> </div> </div>			
TASK DETAILS: ADD DEVICE			
Add Device			
STATUS	UNIT NAME	UNIT TYPE	STATUS DESCRIPTION
	NY_10.1.1.1	Device	Action completed - Action Complete
	NY_10.1.1.2	Device	Action completed - Action Complete
	NY_10.1.1.3	Device	Action completed - Action Complete
	NY_10.1.1.4	Device	Action completed - Action Complete
	NY_10.1.1.5	Device	Action completed - Action Complete
	NY_10.1.1.6	Device	Action completed - Action Complete
	NY_10.1.1.7	Device	Action completed - Action Complete

The Tasks page allows the operator to determine if a task was performed successfully, or, if it's incomplete, what percentage is complete and what percentage remains to be completed.

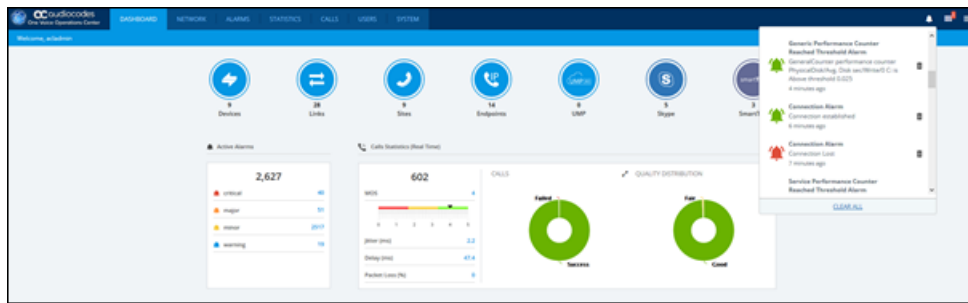
➤ **To view the notifications history:**

1. Click the bell icon in the uppermost right corner of the OVOC GUI.



The bell icon indicates the number of notifications that have not yet been viewed.

2. View the tasks history. In the list, you can delete a notification, delete all notifications or click a notification to open the Tasks page.



3. Scroll down to view earlier notifications. Most recent notifications are listed first. Every notification indicates how long ago it was listed, e.g., **4 minutes ago**.

## 4 Defining your Network Topology

The OVOC enables you to define the topology of your telephony network.



When configuring entities (for example, when adding a device):

- fields and tabs with missing or incomplete information are outlined in red
- fields currently being edited are highlighted yellow
- mandatory fields are marked with an asterix \*

### Adding a Tenant

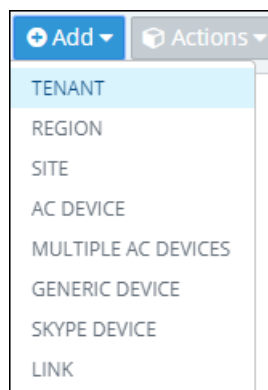


See [Network Architecture](#) on page 2 for details on multi-tenancy vs. non multi-tenancy architecture.

#### ➤ To add a tenant:

1. In the Network page, click **Add**.

**Figure 4-1: Add Tenant**



2. Select **Tenant**.

**Figure 4-2: Tenant Details - General**

×
TENANT DETAILS

GENERAL
SNMP
HTTP
MULTITENANCY
LICENSE

Tenant Name \*

Is Default

License Pool Operator

Description

Subnet (CIDR Notation)

False

▼

3. Use the following table as reference when configuring the tenant's General parameters.

**Table 4-1: Tenant Details - General**

Parameter	Description
Tenant Name	Enter an intuitive name to facilitate effective management later.
Is Default	Defines the default tenant. Only one tenant can be the default. The default is used for devices/endpoints auto-detection.
License Pool Operator	This drop-down list shows all the 'tenant' operators with Admin privileges assigned to this tenant. To manage the Fixed License Pool, it is mandatory to select one of these 'tenant' operators from the drop-down (see also <a href="#">Managing Device Licenses in the Fixed License Pool</a> on page 134). After selecting a 'tenant' operator, the association cannot be removed (see also <a href="#">Adding a 'Tenant' Operator</a> on page 43) and they're automatically displayed under the <b>Operators</b> tab (see following).
Description	Enter a tenant description to facilitate effective management later.
Subnet (CIDR Notation)	Enter the tenant's subnet mask. Must be in prefix format x.x.x.x/y. For example: 255.255.0.0/16. For any <i>region</i> under the tenant, subnet mask is not mandatory, but if it is configured, its subnet mask must be within the tenant's, for example, 255.255.0.0/1.

4. Click **OK** and then click **SNMP**.

**Figure 4-3: Tenant Details – SNMP v2**

TENANT DETAILS

GENERAL **SNMP** HTTP MULTITENANCY LICENSE

SNMP V2

SNMP Read Community \*

SNMP Write Community \*

Trap Community \*

SNMP V3

Security Name \*

Security Level \*

Authentication Protocol \*

Authentication Key \*

Privacy Protocol \*

Privacy Key \*

5. Use the following table as reference when configuring the SNMP v2 parameters.

**Table 4-2: Tenant Details – SNMP v2**

Parameter	Description
SNMP Read Community	Enter an encrypted SNMP read community string. The default value for the SNMP read community string is taken from the SNMP main template.
SNMP Write Community	Enter an encrypted SNMP write community string. The default value for the SNMP write community string is taken from the SNMP main template.
Trap Community	Enter the Trap Community string to be received as part of the Notification message. The default value for the SNMP trap community string is taken from the SNMP main template.

6. Use the following table as reference when configuring the SNMP v3 parameters.

**Table 4-3: Tenant Details – SNMP v3**

Parameter	Description
Security Name	Enter a name for SNMP v3. Example: OVOC User.
Security Level	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>Authentication and Privacy</b> (default)</li> <li>■ <b>No Security</b></li> <li>■ <b>Authentication</b></li> </ul>
Authentication Protocol	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>SHA</b> (default)</li> <li>■ <b>MDS</b></li> <li>■ <b>No Protocol</b></li> </ul>
Authentication Key	Enter an Authentication Key. The default is taken from main SNMP template.
Privacy Protocol	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>AES 128</b> (default)</li> <li>■ <b>DES</b></li> <li>■ <b>The default is taken from main SNMP template</b></li> </ul>
Privacy Key	Enter a Privacy Key. The default is taken from main SNMP template.

7. Click **OK** and then click **HTTP**.



**Note to users of CloudBond 365, CCE Appliance, UMP and SmartTAP:**

SNMPv2/SNMPv3 account credentials are not automatically configured so you need to manually configure identical settings in the device's Web interface (see the device's documentation for more information).

**Figure 4-4: Tenant Details - HTTP**

8. Use the following table as reference when configuring the HTTP parameters.

**Table 4-4: Tenant Details - HTTP**


Parameter	Description
Device Admin User	Enter the device Web server user name. Example: <b>Admin</b> . Password - "Admin". The default is taken from the main HTTP template.
Device Admin Password	Enter the Web server password. Example: <b>Admin</b> . The default is taken from the main HTTP template.
Connectivity	From the drop-down, select either: <ul style="list-style-type: none"> <li>■ <b>HTTP</b> (default)</li> <li>■ <b>HTTPS</b></li> </ul> The default is taken from main SNMP template.

9. Click **OK** and then click **Multitenancy**.

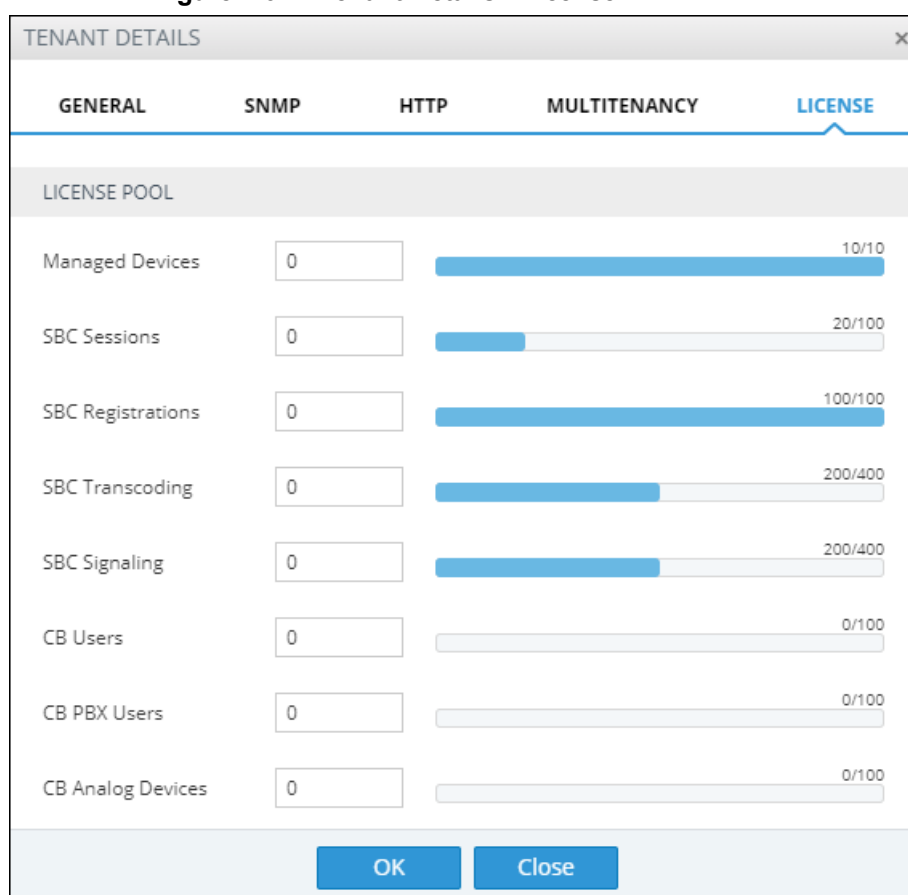
**Figure 4-5: Tenant Details – Multitenancy**

10. Use the following table as reference.

**Table 4-5: Tenant Details - Operators**

Parameter	Description
Local Authentication: Assigned Operators	From the drop-down, select an operator from the list of operators. Only operators configured as 'tenant' type operators are displayed. The list will be empty if no such operator has been configured, in which case you can click the button described next, to add a 'tenant' type operator. The parameter lets you assign an operator – or operators – to the tenant. See <a href="#">Adding a 'Tenant' Operator</a> on page 43 for more information about configuring 'tenant' type operators.
	Operator authentication can be configured locally, in the OVOC (see <a href="#">Configuring Operator Authentication Locally, in the OVOC</a> on page 34). Click the button to add a new 'tenant' type operator; the 'Tenant Operator Details' screen opens (see <a href="#">Adding a 'Tenant' Operator</a> on page 43). The operator is then assigned to the tenant and displayed in the drop-down list.
LDAP Authentication: Group Name	Applies to both 'system' type operators and 'tenant' type operators. When an operator logs in to the OVOC, the OVOC (before allowing the operator access) checks with the enterprise's LDAP server if the User Group which the operator is associated with in the OVOC, tallies with the User Group defined in the LDAP server. If they tally, the operator is authenticated and allowed access. See also <a href="#">Configuring Operator Authentication Centrally using an LDAP Server</a> on page 28.

11. Click **OK** and then click **License**.

**Figure 4-6: Tenant Details - License**


TENANT DETAILS				
GENERAL	SNMP	HTTP	MULTITENANCY	LICENSE
<b>LICENSE POOL</b>				
Managed Devices	<input type="text" value="0"/>	<div><div></div>10/10</div>		
SBC Sessions	<input type="text" value="0"/>	<div><div></div>20/100</div>		
SBC Registrations	<input type="text" value="0"/>	<div><div></div>100/100</div>		
SBC Transcoding	<input type="text" value="0"/>	<div><div></div>200/400</div>		
SBC Signaling	<input type="text" value="0"/>	<div><div></div>200/400</div>		
CB Users	<input type="text" value="0"/>	<div><div></div>0/100</div>		
CB PBX Users	<input type="text" value="0"/>	<div><div></div>0/100</div>		
CB Analog Devices	<input type="text" value="0"/>	<div><div></div>0/100</div>		
		<input type="button" value="OK"/> <input type="button" value="Close"/>		

12. Use the following table as reference when configuring the License parameters.

**Table 4-6: Tenant Details – License**

License Pool	Description
Devices	Enter the total number of devices that can be managed by this tenant's License Pool, i.e., CloudBond 365 devices, SBC devices, gateway devices and MSBR devices allowed by your license. The parameter only defines systems. It does not include phones.
SBC Registrations	Enter the number of SIP endpoints that can register with the SBCs allowed by your license.
SBC Sessions	Enter the number of concurrent call sessions supported by the SBCs in your deployment.
SBC Signaling	Enter the number of SBC signaling sessions supported by the SBCs in your deployment.
SBC Transcoding	Enter the number of SBC transcoding sessions supported by the SBCs in your deployment.
CB Analog Devices	Support pending. Currently unsupported.
CB PBX Users	Support pending. Currently unsupported.
CB Users	Enter the number of CloudBond 365 users per tenant. Divide the total number of CloudBond 365 users allowed by your license, by the number of tenants in your deployment. If you purchased a license for 1000 CloudBond 365 users and you have four tenants in your deployment, 250 users can be allocated to each tenant. You cannot exceed the total number of CloudBond 365 users covered by your license. It's your decision how to distribute them over tenants.
CB Voicemail Accounts	Support pending. Currently unsupported.
<b>Voice Quality</b>	
Devices	Enter the number of SBCs, gateways and MSBRs that can be monitored in this tenant.
Endpoints	Enter the number of endpoints that can be monitored in this tenant.
Sessions	Enter the number of concurrent call sessions the SBCs deployed in this tenant.
Users	Enter the number of users supported by the SBC/s deployed in this tenant.
<b>Endpoints Management</b>	
Endpoints	Enter the number of endpoints the Device Manager application supports for this tenant.

13. Click **OK**; the new tenant is added.

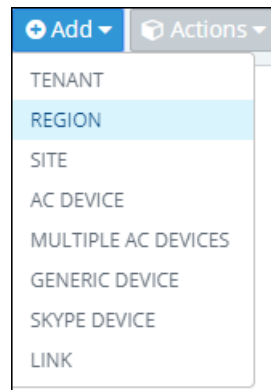
## Adding a Region

ITSPs or enterprises manage devices in regions. A region typically represents a geographical area for the ITSP or the enterprise. Devices are added to the OVOC under a tenant, after defining one.

➤ **To add a region:**

1. Open the Network Topology page (**Network > Topology**).
2. Click **Add** and select Region.

**Figure 4-7: Add Region**



The Region Details screen opens:

**Figure 4-8: Region Details**

 A screenshot of a 'REGION DETAILS' form. The form has a title bar with 'REGION DETAILS' and a close button (X). It contains four input fields: 'Tenant \*' with a dropdown menu showing 'Adi', 'Region Name \*' with a text input field, 'Description' with a larger text input field, and 'Subnet (CIDR Notation)' with a dropdown menu. At the bottom of the form, there are two buttons: 'OK' and 'Close'.

3. From the 'Tenant' drop-down, select a tenant that you configured previously.
4. Define the region's name and type in a description to facilitate operator-friendly management later.
5. [Optional] Enter a subnet mask for the region. If a tenant's subnet mask is 255.255.10.10/16, then the subnet mask of a region under it – if configured – must be *within* that subnet mask, for example: 255.255.10.10/1.
6. Click the now-activated **OK** button; the region is added to the OVOC.

## Adding AudioCodes Devices

AudioCodes devices can be added to the OVOC by:

- **Adding Devices Automatically** (full automatic detection with device-initiated connection) (see Section [Adding AudioCodes Devices Automatically](#) below)
  - Devices are automatically connected to OVOC and added to the default tenant
  - Used predominantly for NAT traversal; allows SNMP communication with devices when they're located behind NAT and OVOC is installed in the WAN
  - Devices initiate the connection to the OVOC and send coldStart and Keep-alive traps to it; OVOC then recognizes each device's IP address and port according to its serial number
- **Adding Devices Manually** from OVOC (OVOC-initiated connection) (see Section [Adding AudioCodes Devices Manually](#) on page 96)
  - **Predefined by IP address:** Devices are manually added to the OVOC by IP address, under the correct entity
  - **Predefined by Serial Number:** Devices are manually added to the OVOC by serial number, under the correct entity
- **Adding Devices with First Time Provisioning** (semi-automatic) (see Section [Enabling Initial Connection Provisioning](#) on page 102)
  - Devices are provisioned with firmware and configuration files for initial connection to OVOC
  - Multiple devices are manually predefined with firmware and configuration files in OVOC
  - Auto detection is then used to connect the devices to OVOC and provision them with these files

## Adding AudioCodes Devices Automatically

Before devices can be managed in the OVOC management interface, they must be added to the OVOC's Network Topology. Devices can be added after acquiring them from AudioCodes, or, as the case may be, after acquiring *the* OVOC from AudioCodes and adding the OVOC to an existing deployment of devices.

The OVOC's Automatic Detection feature enables devices to be *automatically connected and added* to the OVOC without needing to add them manually; when devices are connected to the power supply in the enterprise network and/or are rebooted and initialized, they're automatically detected by the OVOC and added by default to the AutoDetection region.

For this feature to function devices must be:

- configured with the OVOC server's IP address
- configured to send keep-alive messages

The OVOC then connects to the devices and automatically determines their firmware version and subnet. They're then added to the appropriate tenant/region according to the best match for subnet address.

- When a default tenant *exists*, devices that *cannot be successfully matched with a subnet* are added to an automatically created AutoDetection Region under the default tenant
- When a default tenant *does not exist* and the device *cannot be matched with a subnet*, the device isn't added to the OVOC

The Automatic Detection feature is used also for NAT traversal, and allows SNMP communication with the devices when they are located behind a NAT and are managed over a remote WAN connection.



- SNMPv2 or SNMPv3 credentials are configured in the device Web interface. SNMP settings connect the devices and the OVOC. The following figures show the Web interface pages in which these settings are configured. See also the device's *User's Manual* for more information.
- If a device detects the OVOC but the OVOC does not detect the device, the device sends an event to the OVOC; the OVOC takes the information from the event and automatically connects the device.

**Figure 4-9: Web interface: SNMP Community Strings**

The screenshot displays the 'SNMP Community Settings' page in the OVOC web interface. The interface has a blue header with 'ADMINISTRATION' selected. A left sidebar contains a tree view with 'SNMP' expanded, showing 'SNMP Community Settings' as the active page. The main panel is titled 'SNMP Community Settings' and contains three sections:

- GENERAL SETTINGS:** Includes a 'Disable SNMP' dropdown menu currently set to 'No'.
- MISC. SETTINGS:** Includes a 'Trap Community String' text field with the value 'trapuser', a 'Trap Manager Host Name' text field, and an 'Activity Trap' dropdown menu set to 'Disable'.
- READ-ONLY COMMUNITY STRINGS:** A list of five input fields labeled 'Read-Only 1' through 'Read-Only 5'.
- READ-WRITE COMMUNITY STRINGS:** A list of five input fields labeled 'Read-Write 1' through 'Read-Write 5'.

At the bottom right of the main panel, there are 'Cancel' and 'APPLY' buttons.

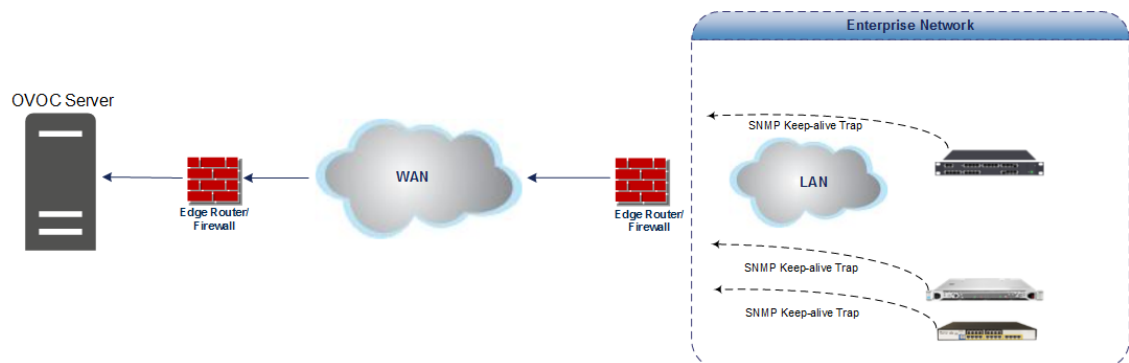
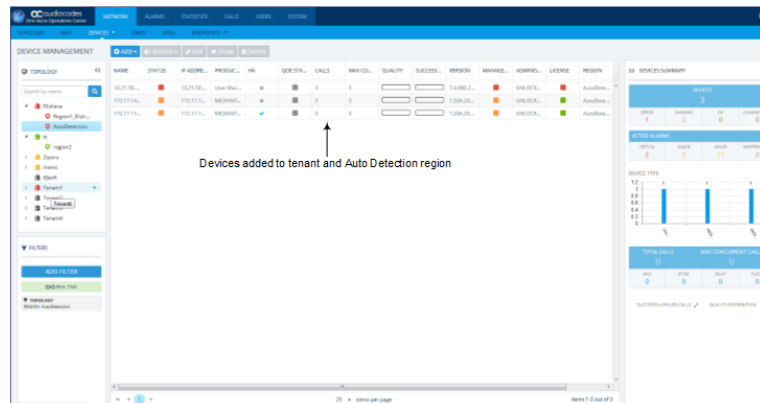
**Figure 4-10: Web interface: SNMP Trap Destinations**

The screenshot shows the 'SNMP Trap Destinations' configuration page in the OVOC web interface. The sidebar on the left contains navigation links: 'TIME & DATE', 'WEB & CLI', 'Local Users (4)', 'Web Settings', 'SNMP', and 'MAINTENANCE'. The 'SNMP' section is expanded, showing 'SNMP Community Settings', 'SNMP Trap Destinations' (selected), 'SNMP Trusted Managers', and 'SNMP V3 Users (0)'. The main content area displays a table of configured trap destinations.

	NAME	IP ADDRESS	TRAP PORT	TRAP USER	TRAP ENABLE
<input checked="" type="checkbox"/>	SNMP Manager 1	172.17.140.203	162	v2cParams	Enable
<input type="checkbox"/>	SNMP Manager 2	0.0.0.0	162	v2cParams	Enable
<input checked="" type="checkbox"/>	SNMP Manager 3	10.3.180.235	162	v2cParams	Enable
<input checked="" type="checkbox"/>	SNMP Manager 4	10.3.180.13	162	v2cParams	Enable
<input checked="" type="checkbox"/>	SNMP Manager 5	172.17.140.84	162	v2cParams	Enable

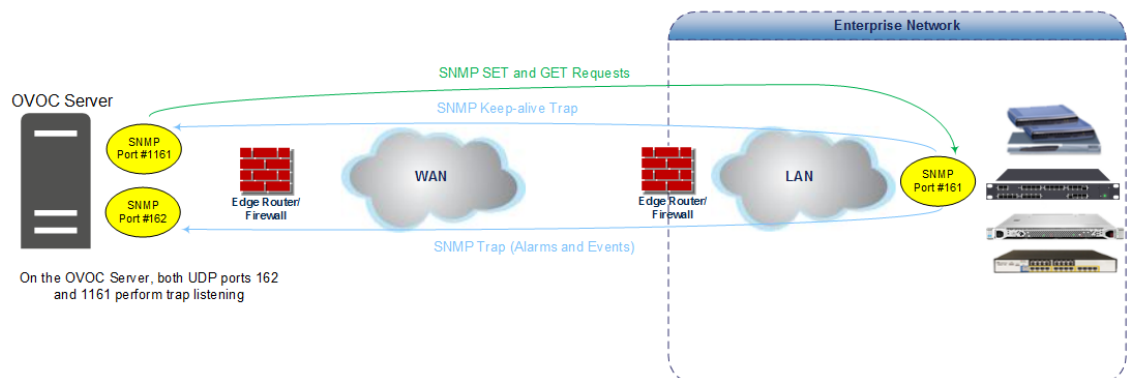
At the bottom of the page, there are 'Cancel' and 'APPLY' buttons.

When devices are deployed in a private network using Network Address Translation (NAT), they can connect to the internet so long as their connection with the OVOC server is alive. You consequently need to configure devices to send coldStart (after device reset) and keep-alive traps (sent every 30 seconds by default) to the OVOC server. This allows the OVOC to perform SNMP SET and GET commands at any time. When devices are added to the OVOC, the OVOC recognizes them according to their field 'sysDesc' and their serial number, and according to the entries in the OVOC database. A device's default name comprises the router's IP address and the port number. The NAT sometimes changes device IP address and port. The OVOC recognizes these changes after devices are reset.

**Figure 4-11: AudioCodes Devices Added to OVOC**

The following figure illustrates SNMP connectivity between OVOC and AudioCodes devices:

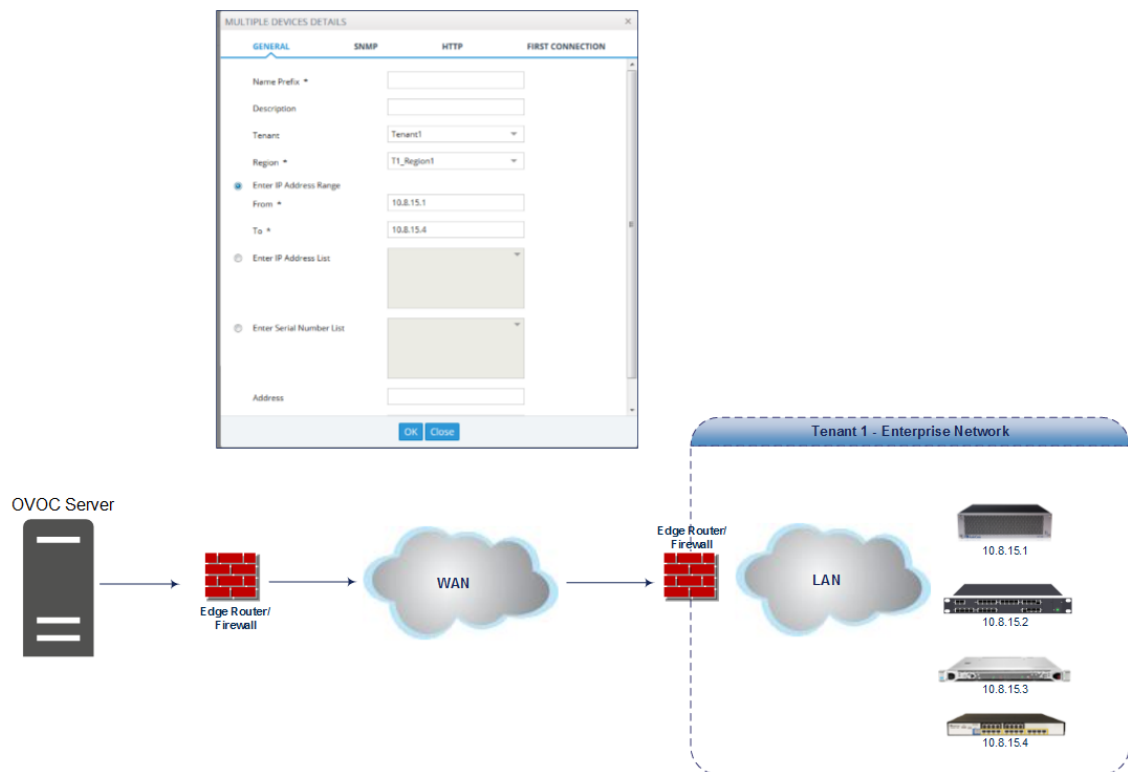
- UDP ports 162 and 1161 on the OVOC server are configured to listen for traps from AudioCodes devices
- UDP port 1161 on the OVOC server sends SNMP SET requests to AudioCodes devices

**Figure 4-12: OVOC Server and Devices SNMP Connections**

## Adding AudioCodes Devices Manually

When *manually* adding an AudioCodes device - or multiple AudioCodes devices - to the network for the first time, you can enable 'Initial Connection Provisioning' a.k.a. First Time Provisioning, for devices to automatically be provisioned with their firmware and configuration files. The figure following shows an example of manually adding multiple AudioCodes devices to OVOC.

**Figure 4-13: Manually Adding Multiple AudioCodes Devices to OVOC**



### ➤ To manually add the devices:

1. Open the Network Topology page (**Network > Topology**).
2. Click **Add** and select **AC Device** or **Multiple AC Devices**.

**Figure 4-14: AC Device | Multiple AC Devices**



The Device Details screen opens under the **General** tab:

**Figure 4-15: Device Details – General**

AUDIO CODES DEVICE DETAILS

**GENERAL**    SNMP    HTTP    FIRST CONNECTION    SBA

Name \*

Description

Tenant    Adi

Region \*    Israel

☐ FQDN

☒ IP Address \*

☐ Serial Number 1

Serial Number 2

Address

OK    Close

3. Define an intuitive device name to facilitate operator-friendly management later. Do not use underscores in the name.
4. Provide a description of the device to facilitate operator-friendly management later.
5. From the 'Tenant' drop-down, select a tenant that you configured as shown in [Adding a Tenant](#) on page 85.
6. Select the region under which the device is located.
7. Define the device by selecting one of these three options (refer to the figures above):
  - Select and enter the device's **IP address**. If selected, the 'FQDN' and 'Serial Number' fields will be disabled and the device will immediately be connected to the OVOC. If you're adding **Multiple AC Devices**, you need to enter the IP Address *range* in the fields that will be displayed.
  - Select and enter the device's **FQDN**. If selected, the 'IP Address' and 'Serial Number' fields will be read-only). This option allows performing SBC SSO in a way that the URL includes only FQDN names (OVOC & SBC) rather than IP addresses.



- If a device is defined using FQDN and the OVOC cannot resolve the IP address, the OVOC will not be able to manage the device until the IP address is resolved. The same applies to the Add and Refresh processes.
- FQDN is not editable after a device is defined using the FQDN option. Same applies to IP Address and Serial Number – they are not editable after defining the device using them.
- The FQDN option is not supported when adding multiple devices.
- Devices behind a NAT and devices added as a result of a keep-alive trap (auto detection) are managed using IP address + port (rather than FQDN).
- Alarm Forwarding is performed using IP address.

- [Optional] Select and enter the device's **Serial Number**. If selected, the 'FQDN' and 'IP Address' fields will be read-only. You can get the SN from the device's Web interface's Information page. The SN is only necessary for auto-detection. Generally, it is not mandatory to enter the serial number when adding a device.
8. [Optional] In the 'Address' field, enter the first letters in the name of the city / country in which to locate the device, and then select the city / country from the list that pops up.
  9. You need to configure the device's SNMP settings if you're connecting the device to the OVOC.
    - To configure SNMPv2, click the **SNMPv2** tab:

**Figure 4-16: Device Details – SNMP v2**

MULTIPLE AUDIO CODES DEVICES DETAILS

GENERAL **SNMP** HTTP FIRST CONNECTION

☒ SNMP v2 ☐ SNMP v3

SNMP Read Community

SNMP Write Community

OK Close



Before connecting a device to the OVOC, an SNMP connection between the device and the OVOC must be configured. SNMP is used to establish an initial connection with the device for provisioning and in addition, for daily operations, including maintenance actions and fault and performance management.

SNMPv3 provides more sophisticated security mechanisms than SNMPv2c. It implements a user-based security model (USM), allowing both authentication and encryption of the requests sent between the OVOC and agents, as well as user-based access control.

The SNMP connection must be configured on both the OVOC and the device. SNMP parameters include

- specifying the IP address of the OVOC server. All traps are sent from the device to this address. For establishing the connection with the OVOC, this is the destination address for the coldStart and Keep-alive traps.
- associating an SNMPv2 or SNMPv3 trap user with the OVOC server destination. The Keep-alive trap indicates whether the device is configured for SNMPv2 or SNMPv3. The configured SNMPv2 or SNMPv3 user credentials are verified with the following default OVOC configuration:
  - ◆ SNMPv2: SNMPReadCommunity string 'public' and SNMPWriteCommunity string 'private' and Trap User 'trapuser'
  - ◆ SNMPv3: User 'OVOCUser'; Auth protocol 'SHA'; Privacy protocol 'AES-128'; password '123456789'

Identical SNMP parameter values must be configured on the device and in the OVOC. If different values are configured on the device, it's added to the OVOC as 'Unknown' until updated in the OVOC. The defaults under the SNMP tab are taken from the SNMP tenant profile.

- ◆ Enter the device's SNMP Read and Write Community strings.
- To configure SNMPv3, select the **SNMP v3** option:

**Figure 4-17: Device Details – SNMP v3**


The OVOC can automatically add up to 255 devices at a time after SNMP credentials and other device settings are configured and functioning correctly.

- a. In the 'Security Name' field, enter the Security name of the SNMPv3 operator.
- b. From the 'Authentication Protocol' drop-down, select an authentication protocol. The corresponding security level is displayed in the 'Security Level' field.
- c. In the 'Authentication Key' field, leave the default unchanged or enter an authentication password.
- d. From the 'Privacy Protocol' drop-down, leave the default unchanged or select a Privacy Protocol.
- e. In the 'Privacy Key' field, leave the default unchanged or enter a privacy password.

The defaults are taken from the SNMP tenant profile.

10. Click the now-activated **OK** button or click the **HTTP** tab.

**Figure 4-18: AudioCodes Device Details – HTTP**

AUDIO CODES DEVICE DETAILS

GENERAL    SNMP    **HTTP**    FIRST CONNECTION    SBA

Device Admin User: Admin

Device Admin Password: \*\*\*\*\*

Enable HTTPS Connection: ☐

OK    Close



The defaults are taken from the HTTP tenant profile.

11. [Optional] In the 'Device Admin User' field, enter the device's web server user name and in the 'Device Admin Password' field, enter the web server password.  
Example: **Admin, Admin**.
12. To secure the connection with the device, select the **Enable HTTPS Connection** option.  
Securing the connection between the OVOC server and the AudioCodes device over HTTPS is used for files upload/download and for Web Client Single-Sign On.



- You can also configure HTTPS on the AudioCodes device (see the *Server IOM* for more information).
- You can also secure the connection using the default AudioCodes self-signed certificate or load custom certificates to the OVOC server (see the *Server IOM* for more information).
- To operate in 'Mutual Authentication' mode:
  - ✓ Set the HTTPS Authentication option 'Set Mutual Authentication' using the OVOC Server Manager (see the *Server IOM*).
  - ✓ Load certificates to the device (you must use the same root CA for signing the device certificate as is used for signing the certificate installed on the OVOC server) (see 'Custom X.509 Certificates - Supplementary Procedures' in the *Server IOM*).
  - ✓ Configure HTTPS on the device (see 'Custom X.509 Certificates - Supplementary Procedures' in the *Server IOM*).

13. Click the now-activated **OK** button or click the **SBA** tab.

**Figure 4-19: AudioCodes Device Details – SBA**

The screenshot shows a dialog box titled "AUDIO CODES DEVICE DETAILS" with a close button (X) in the top right corner. The dialog has five tabs: GENERAL, SNMP, HTTP, FIRST CONNECTION, and SBA. The SBA tab is currently selected and highlighted with a blue underline. Inside the SBA tab, there is a checkbox labeled "Enable SBA" which is currently unchecked. Below this, there are two radio buttons: "IP Address" (which is selected) and "FQDN Name". To the right of these radio buttons are two text input fields. Below the radio buttons, there are three more text input fields labeled "SNMP Read Community", "SNMP Write Community", and "Description". At the bottom of the dialog, there are two buttons: "OK" and "Close".

14. Select the **Enable SBA** option. This is only relevant if the device contains an SBA module.
15. Enter the IP address of the SBA Management Interface –OR- select the 'FQDN Name' option and in the field 'FQDN Name', enter the FQDN (Fully Qualified Domain Name) of the SBA.  
Example: **HOST/Branch01.SFB.interop**
16. Enter an encrypted SNMP read community string.
17. Enter an encrypted SNMP write community string.
18. Enter a description to facilitate an operator-friendly management experience later.
19. Click the now-activated **OK** button or click the **First Connection** tab.



After adding a SmartTAP device to the OVOC, it's Unknown until the SmartTAP Agents have been installed on the SmartTAP Server because the Keep-alive mechanism is managed by these agents. See also the *SmartTAP Installation Manual*.

## Enabling Initial Connection Provisioning

After acquiring a device - or multiple devices - from AudioCodes, you can add them to the OVOC. You can opt to enable 'Initial Connection Provisioning' a.k.a. First Time Provisioning, for devices to *automatically* be provisioned with their firmware and configuration files, rather than manually, after they're connected to from the OVOC.

### ➤ To enable 'Initial Connection Provisioning' a.k.a. First Time Provisioning:

1. Click the **First Connection** tab and then select the option 'Enable Initial Connection Provisioning'; this enables the device/s to automatically be provisioned with their firmware and configuration files when they are connected to the OVOC server for the first time.

**Figure 4-20: AudioCodes Device Details – First Connection**

2. From the now-activated 'Configuration File' drop-down, select the applicable file.
3. From the now-activated 'Firmware File' drop-down, select the applicable file.



The configuration and firmware files must be prepared and located in the OVOC's Software Manager. See [Adding Configuration Files to the OVOC's Software Manager](#) for more information.

4. Click the now-activated **OK** button; the devices are added to the OVOC.



The AudioCodes Mediant 2000 Media Gateway device housing two TP-1610 blades can be added to OVOC using a single IP address rather than using two IP addresses (one for each blade) as was the case in OVOC versions earlier than Version 7.4.3000. Existing customers must remove any Mediant 2000 device housing two TP blades that was added to the OVOC using two IP addresses in OVOC versions earlier than Version 7.4.3000, and then add them again using a single IP address. After this action, the Alarms History and QoE calls & statistics history is cleared.

In a related scenario, you can add OVOC to an *existing* deployment after acquiring the OVOC *later*.

## Before Enabling the Feature

Before enabling Initial Connection Provisioning, you need to validate the ini file.

### ➤ To validate the ini file:

1. Access each device using its default IP address directly through the Web interface or CLI, and then configure its network settings (e.g., OAMP IP address) so that it suits your network environment. Network settings are configured in these tables:
  - IP Interfaces
  - Ethernet Device
  - Ethernet Group
  - Physical Ports
  - Static Route
  - QoS Settings
2. Make sure the IP Interfaces table's indexes, names and application types *are identical* for each device so that the template configuration file will be applied to all devices in the network. In the validation process, each index entry is validated with the equivalent entry in the template file (see [Interfaces Table Excerpted from the ini File](#) below for a file example).



If any device's IP interface table does not meet these requirements, the Initial Connection Provisioning will fail and an alarm will be sent to the OVOC (see [Making Sure First Time Provisioning was Successful](#) on page 106).

## Interfaces Table Excerpted from the ini File

The following example shows an example of a device's ini file's IP Interfaces table parameters. Validated values are displayed in blue. Not validated values are displayed in red and are only read from the device once the blue parameters are successfully validated.

```
[ \InterfaceTable ]
```

```
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_
InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_
Gateway, InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingDevice;
```

```
InterfaceTable 0 = 6, 10, 10.15.17.10, 16, 10.15.0.1, "Voice", 10.15.25.1, 0.0.0.0, "vlan 1";
```

```
InterfaceTable 1 = 5, 10, 195.189.192.156, 25, 195.189.192.129, "WANSP", 80.179.52.100,
80.179.55.100, "vlan 2";
```

## Enabling the Feature

The Initial Connection Provisioning feature is implemented by the **First Connection** tab shown in the following figure (on the left) - when adding a single AudioCodes device - and in the figure following (on the right) when adding multiple AudioCodes devices.



Before adding a device or multiple devices, you must load the device ini and .cmp files to the OVOC's Software Manager. See [Adding Configuration Files to the OVOC's Software Manager](#) on page 72 for details.

**Figure 4-21: First Connection: Add AudioCodes Device**

MULTIPLE DEVICES DETAILS

GENERAL

SNMP

HTTP

FIRST CONNECTION

Enable Initial Connection Provisioning ☒

Configuration File (INI/CLI/CONF) \*

BOARD\_SN10465144 (11).ini ...

Firmware File (CMP/RMS/RMT)

M1000\_SIP\_F6.60A.337.002.c...

Firmware Version

6.60A.337.002

Supporting Products

MEDIANT\_1000

MEDIANT\_600

OK

Close

**Figure 4-22: First Connection: Add Multiple AudioCodes Devices**

The dialog box titled "ADD MULTIPLE DEVICES" has a close button (X) in the top right corner. It features four tabs: "GENERAL", "SNMP", "HTTP", and "FIRST CONNECTION", with the last tab being active. Below the tabs, there is a checkbox labeled "Enable Initial Connection Provisioning". Underneath this checkbox are four fields: "Configuration File (INI/CLI/CONF)", "Firmware File (CMP/RMS/RMT)", "Firmware Version", and "Supporting Products". Each of these four fields has a corresponding dropdown menu icon (a downward arrow) to its right. At the bottom of the dialog, there are two buttons: "OK" and "Cancel".

➤ **To enable the feature:**

- Make sure the **Enable Initial Connection Provisioning** option shown in the figures above is selected.

See also [Adding AudioCodes Devices Automatically](#) on page 92 for related information.

## Making Sure First Time Provisioning was Successful

The Journal page helps you confirm that the configuration and firmware files were automatically loaded to the device after the device is connected to the network.

➤ **To make sure first time provisioning was successful:**

1. Open the Journal page (**Alarms > Journal**).

**Figure 4-23: Alarms Journal**

JOURNAL

FILTERS <<

ADD FILTER

REAL TIME

MORE FILTERS

Actions

Refresh

SEV...	DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION	TENANT	OPERATOR
	30-Jul-17 11:48:12	AutoDetection		CONFIGURATION_ADD	Add Region: AutoDetection in tenant Singapore	Singapore	InternalSystem
	30-Jul-17 11:45:53	System		CONFIGURATION_RE...	Endpoint name 009085FF9BA, 192.168.3.124 was deleted	AudioCodes	Internal System
	30-Jul-17 11:35:04	Singapore		CONFIGURATION_UP...	Singapore tenant was updated.Tenants subnet masks was changed fro...	Singapore	shai
	30-Jul-17 11:34:43	Singapore		CONFIGURATION_UP...	Singapore tenant was updated.	Singapore	shai
	30-Jul-17 11:31:11	Singapore		CONFIGURATION_ADD	New Tenant Singapore was added.	Singapore	shai
	30-Jul-17 11:30:53	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.38.2.9 with Administration security leve...	System	shai
	30-Jul-17 11:29:23	System	EMS Server	SECURITY_EDIT_OPE...	Update email user details: password was changed to *****;	System	shai
	30-Jul-17 11:29:23	System	EMS Server	SECURITY_EDIT_OPE...	Changing user password: email	System	shai
	30-Jul-17 11:27:42	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.16.2.10 with Administration security lev...	System	shai
	30-Jul-17 11:27:06	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.1.1.11 with Administration security lev...	System	shai

JOURNAL ALARM DETAILS

GENERAL INFO

ENTITY INFO

USER INFO

SEVERITY

DATE AND TIME

ACTION TYPE

SOURCE

UNIQUE ID

DESCRIPTION

Journal

30-Jul-17 11:48:12

CONFIGURATION\_ADD

6683

Add Region: AutoDetection in tenant Singapore

2. Optionally filter the page by Time Range (see [Filtering to Access Specific Information](#) on page 147), Topology (see [Filtering by 'Topology'](#) on page 150), Source Type (see [Filtering by 'Severity'](#) on page 158) or More Filters (see [Filtering the Alarms Journal by 'More Filters'](#) on page 164).
3. Locate and select the First Time Provisioning / Initial Connection Provisioning alarm.
4. In the Journal Alarm Details pane on the right side of the page, click the **Entity Info** tab.

Figure 4-24: Alarms Journal – Entity Info

JOURNAL								
FILTERS <<		SEV...	DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION	TENANT
ADD FILTER			30-Jul-17 11:58:22	009085FF6BA...		CONFIGURATION_UP...	Endpoint null, update fields: TENANT ID = 79117	Singapore
OIO REAL TIME			30-Jul-17 11:55:59	System	EMS Server	SECURITY_LOGIN	shai logged in via OVOC from 10.1.1.117 with Administration security lev...	Internal System
MORE FILTERS			30-Jul-17 11:48:12	AutoDetection		CONFIGURATION_ADD	Add Region: AutoDetection in tenant Singapore	System
			30-Jul-17 11:45:53	System		CONFIGURATION_RE...	Endpoint name 009085FF6BA, 192.168.3.124 was deleted	Internal System
			30-Jul-17 11:35:04	Singapore		CONFIGURATION_UP...	Singapore tenant was updated. Tenants subnet masks was changed fro...	AudioCodes
			30-Jul-17 11:34:43	Singapore		CONFIGURATION_UP...	Singapore tenant was updated.	Internal System

5. If Initial Connection Provisioning was unsuccessful, you'll view the following:

Figure 4-25: Critical Alarm – Initial Connection Provisioning Failed

SEVERITY						ALL ALARM DETAILS		
RECEIVED DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION		ALARM INFO	MG INFO	SNMP INFO
24-Jul-17 16:47:04	11.200.1.2	EMS Server/11.200.1.2	Pre-Provisioning	Pre-Provisioning Process Failed: Device Name: 11.200.1.2, Device IP: 11.200.1.2, Device ...		ALARM NAME	Pre-Provisioning	
24-Jul-17 16:46:58	11.200.1.2	EMS Server	Topology Update	Update GW		SEVERITY	Critical	
24-Jul-17 16:46:58	11.200.1.2	EMS Server	GW Connection Alarm	Connection established		OCCURRED DATE AND TIME	24-Jul-17 16:47:04	
						RECEIVED DATE AND TIME	24-Jul-17 16:47:04	
						SOURCE	EMS Server/11.200.1.2	
						SOURCE DESCRIPTION		
						UNIQUE ID	7	
						ALARM TYPE	OPERATIONALVIOLATION	
						PROBABLE CAUSE	CONFIGURATIONORCUSTOMIZATIONERROR	
						DESCRIPTION	Pre-Provisioning Process Failed: Device Name: 11.200.1.2, Device IP: 11.200.1.2, Device S/N: 2.	
						ADDITIONAL INFO 1	Predefined INI File: null. Reason: CMP file does not match device product type.	
						ADDITIONAL INFO 2		
						ADDITIONAL INFO 3	11.200.1.2	



If Initial Connection Provisioning was unsuccessful, download the configuration or firmware file to the device as shown in [Backing Up](#) on page 212.

After an ini or cmp file is deployed on multiple devices, you may need to customize one device's configuration to suite specific requirements.

➤ **To change the .cmp or ini file after successfully automatically provisioning a device:**

- Remove the device from the OVOC and then add it again. When the device is removed, the OVOC server IP address in the Trap Destination Rule is reset to 0.0.0.0, so when you add the device again you need to reconfigure this IP address in the SNMP Trap Destinations table. See the relevant *SIP User's Manual* for more information.



AudioCodes recommends that you consult with AudioCodes Customer Support or Professional Services about special configuration issues.

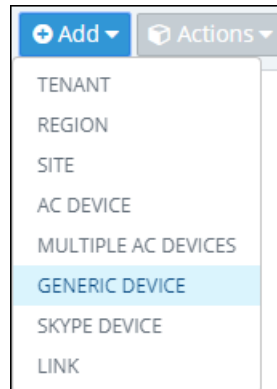
## Adding a Generic Device Manually

A generic (non-AudioCodes) device can manually be added to the OVOC.

➤ **To manually add a generic device:**

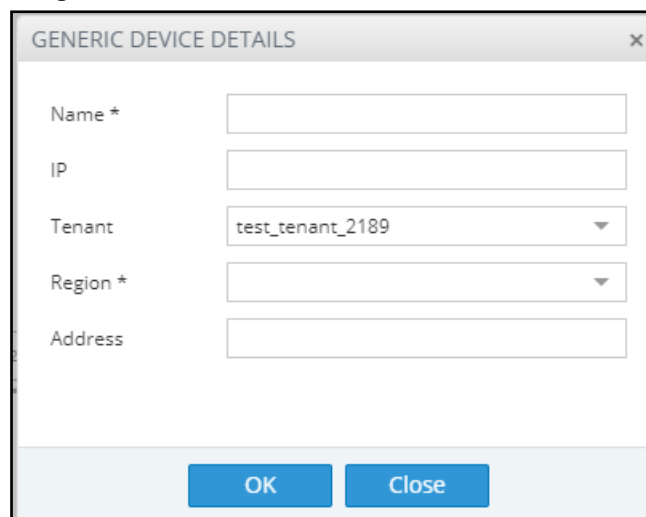
1. Open the Network Topology page (**Network > Topology**).
2. Click **Add** and select **Generic Device**.

**Figure 4-26: Add Generic Device**



The Generic Device Details screen opens:

**Figure 4-27: Generic Device Details**

A screenshot of a 'GENERIC DEVICE DETAILS' form. The form has a title bar with a close button (X). It contains several input fields: 'Name \*' (text input), 'IP' (text input), 'Tenant' (dropdown menu with 'test\_tenant\_2189' selected), 'Region \*' (dropdown menu), and 'Address' (text input). At the bottom of the form are two buttons: 'OK' and 'Close'.

3. Define an intuitive device name to facilitate operator-friendly management later. Do not use underscores in the name.
4. Enter the device's IP address.
5. From the 'Tenant' drop-down, select the device's tenant.
6. From the 'Region' drop-down, select the device's region and then click the now-activated **OK** button; the device is added and displayed in the OVOC.

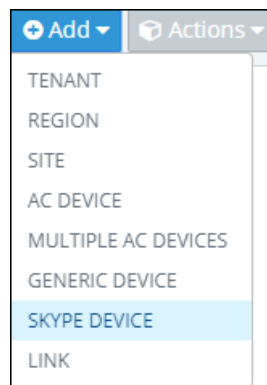
## Adding a Microsoft Skype for Business Device Manually

The most commonly used Microsoft device is Microsoft Skype for Business server. The OVOC can calculate, for example, call quality for the link defined between AudioCodes devices and Microsoft Skype for Business server. See also [Adding an Unprivileged User to MSSQL Server](#) on page 291.

➤ **To add a Microsoft Skype for Business device:**

1. Open the Network Topology page (**Network > Topology**).
2. Click **Add** and select **Skype Device**.

**Figure 4-28: Add Skype Device**



The Skype Details screen opens.

Figure 4-29: Skype Details

**SKYPE DETAILS**

Name \*

Tenant ErezTenantz

Region \* ErezRegion

Device Type Front End Server

FQDN \*

Address

---

SQL SERVER DB

IP Address \*

☒ Port \* 1433

☐ Instance Name

Connection Mode SQL Server Authentication

Username \*

Password \*

SSL DISABLED

OK Close

3. Define an intuitive name to facilitate operator-friendly management later. Don't use underscores.
4. From the 'Region' drop-down, select a region you configured when [Adding a Region](#) on page 91.
5. From the 'Device Type' drop-down, select:
  - **Microsoft Skype for Business FE (Front End) Server**
    - ◆ The main FE parameters are 'NAME' and 'FQDN'. Other SQL parameters are for the SQL Skype for Business Database.
    - ◆ FE Server points/reports to the SQL Database. It does not point/report to the Skype for Business FE Services.
    - ◆ The SEM server connects to the SQL Monitoring Server and pulls control and media information from it for display.
  - **Microsoft Skype for Business Mediation Server**
    - ◆ Implements enterprise voice and dial-in conferencing
    - ◆ Translates signaling and media (in some configurations) between your internal Skype for Business Server infrastructure and a public switched telephone network (PSTN) gateway, IP-PBX, or a Session Initiation Protocol (SIP) trunk
  - **Microsoft Skype for Business Edge Server**
    - ◆ Deployed in a DMZ
    - ◆ Provides access to the Skype for Business system from the Internet

- ◆ Lets your users communicate with users outside the enterprise firewall
  - **Microsoft Skype for Business SBA (Survivable Branch Appliance)**
    - ◆ Ensures access to data and voice services in the event of a WAN outage
6. In the 'FQDN' field, enter the device's Fully Qualified Domain Name.
  7. Under the SQL Server DB section, enter in the 'IP Address' field the IP address of the SQL Server. Applies to the centralized Skype for Business database.



Microsoft Skype for Business Server for customers with multiple FrontEnd servers and one SQL server.

- Up to two Microsoft Skype for Business solutions in one OVOC application.
- Microsoft Skype for Business Server limitation: When functioning with Skype for Business server pools (FE, Edge and Mediation), the FE server defined in the OVOC functions as the monitoring SQL database. After connecting, the OVOC presents all Call Details from the Skype for Business network in the OVOC's Calls List and Call Details views. When functioning with Skype for Business pools, FE, Edge and Mediation servers cannot be defined in the OVOC, so the entire Skype for Business network is presented in the OVOC only as a single object, namely, the monitoring SQL database.

8. Select either the:
  - 'SQL Port' option and in the now-activated field enter the port number of the SQL Server. Applies to the centralized Skype for Business database.
  - 'SQL Instance Name' option (by default selected)
9. [Optional] From the 'Connection Mode' drop-down, select:
  - **Windows Authentication** to allow the connection between the MS-SQL Server (Microsoft Front End) and the OVOC Server to be authenticated using a Windows user's credentials (password and user)
  - **SQL Server Authentication** (default) to allow the connection between the MS-SQL Server (Microsoft Front End) and the OVOC Server to be authenticated using the SQL Server user's credentials
10. In the 'User Name' field, enter the user of the SQL Server or Windows Server. Applies to the centralized Skype for Business database.
11. In the 'Password' field, enter the Password of the SQL Server or Windows Server. Applies to the centralized Skype for Business database.
12. In the 'Domain' field (relevant only when 'Connection Mode' is configured to **Windows Authentication**), enter the Windows Server user's domain.
13. From the 'SSL' drop-down, secure the connection between the OVOC and the SQL server over SSL by selecting either:
  - **Trusted:** An SSL connection between the OVOC server and the SQL server is opened, though it's not authenticated using a certificate.
  - **Using Certificate:** An SSL connection between the OVOC and the SQL server is opened. The OVOC authenticates the SSL connection using a certificate. Make sure you load the SSL certificate file, required by the SQL server, to the Software Manager. See [Adding Configuration Files to the OVOC's Software Manager](#) on page 72.

Default: **Disabled**. The SSL connection with the SQL server is by default non-secured.
14. [Optional] In the 'Address' field, enter the first letters in the name of the city / country in which to locate the device, and then select the city / country from the list that pops up.
15. Click the now-activated **OK** button; the Skype for Business device is added.

## Backing up a Device's Configuration using Backup Manager

You can manually back up a device's configuration to the OVOC server using the Backup Manager. For details on configuring automatic periodic device configuration backups, see [Enabling Automatic Device Backup Periodically](#) on page 80.

### Manually Backing up a Device's Configuration

The Backup Manager page lets you manually back up a device configuration on the server.

➤ **To manually back up a device's configuration on the OVOC server:**

1. In the OVOC, open the Backup Manager page (**Network > Devices > Backup Manager**).

**Figure 4-30: Backup Manager**

BACKUP MANAGER

Actions

REGIONS

FILTERS

ADD

Enter search string

aa

Chaya

Zipora

t1

Zvi\_T

Backup summary

DEVICE NAME	PRODUCT TY...	NUMBER OF ...	LAST SUCCES...	LAST BACKU...	LAST BACKU...	REGION	TENANT
172.17.140.1...	Mediant 800 ...	6	19-Nov-17 04:00	19-Nov-17 04:00	SUCCESS UP...	bb	aa
10.3.181.96	SW SBC	5	19-Nov-17 04:00	19-Nov-17 04:00	SUCCESS UP...	HA region	Zipora
172.17.116.93	MEDIAN 80...	2	16-Nov-17 04:00	19-Nov-17 04:00	FAIL NOT CO...	region_1	Chaya
10.3.151.247	SW SBC	5	19-Nov-17 04:00	19-Nov-17 04:00	SUCCESS UP...	Zvi_R	Zvi_T

Backup Files

BACKUP TYPE	UPLOAD TIME	FILE TYPE	FILE SIZE	FILE NAME
PERIODIC	15-Nov-17 04:00:27	INI	13301	1561510711227054_10...
PERIODIC	16-Nov-17 04:00:21	INI	13301	1561510797621756_10...
PERIODIC	17-Nov-17 04:00:16	INI	14965	1561510884016795_10...
PERIODIC	18-Nov-17 04:00:16	INI	14965	1561510970416805_10...
PERIODIC	19-Nov-17 04:00:16	INI	14965	1561511056816769_10...
MANUAL	15-Nov-17 14:23:34	INI	25598	32281510748614100_1...
PERIODIC	16-Nov-17 04:00:16	INI	25602	32281510797616435_1...
MANUAL	15-Nov-17 15:18:30	INI	27681	32321510751910108_1...
PERIODIC	16-Nov-17 04:00:05	INI	27715	32321510797605495_1...
PERIODIC	17-Nov-17 04:00:05	INI	27605	32321510884005899_1...
PERIODIC	18-Nov-17 04:00:05	INI	27605	32321510979040589_1...
PERIODIC	19-Nov-17 04:00:05	INI	27605	32321511056805882_1...
MANUAL	07-Nov-17 10:44:34	CLI SCRIPT	8175	55151004274646_172...
PERIODIC	12-Nov-17 04:00:11	CLI SCRIPT	8187	5515104032011326_172...
PERIODIC	14-Nov-17 04:00:11	CLI SCRIPT	8175	551510634811908_172...
PERIODIC	15-Nov-17 04:00:15	CLI SCRIPT	8175	551510711215367_172...
PERIODIC	18-Nov-17 04:00:11	CLI SCRIPT	8187	551510970411470_172...
PERIODIC	19-Nov-17 04:00:11	CLI SCRIPT	8187	551511056811449_172...

The Backup Manager page displays:

- **Backup Summary** pane: For all files that have been backed up to the OVOC for each device.
- **Backup Files** pane: Full list of all the backup ini and CLI script (MSBR devices files) for CPE devices files that have been saved to the Backup Manager for all devices.

Each entry in the summary displays:

- Device Name and Product Type
- The number of files backed up from the device to the OVOC
- The last backup status, e.g., Successful
- The date of the last backup file
- The tenant under which the device is located

You can filter displayed files for more effective access to the specific files you need:

- Click a column header; files are displayed accordingly.

Backed-up file names are in the format:

node id|timestamp \_ Device IP Address \_ Node ID \_ Serial Number \_ periodic/manual \_ Product type \_ INI/CONF/CLI \_ Date Formatted

Here's an example of a backed-up filename:

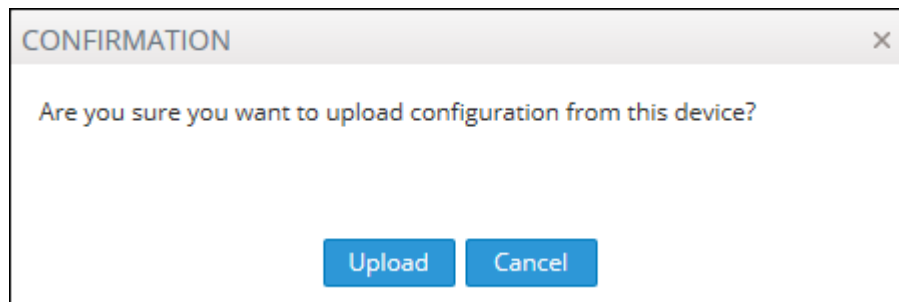
*411515387481228\_192.168.200.47\_41\_3968002\_m\_82\_INI\_TYPE\_2258-Jan-07-2018.ini*

Use the following table as reference to the example.

**Table 4-7: Explanation of Backed Up File Name Format**

File Name Format	Explanation
411515387481228	Indicates the Node ID  Timestamp
192.168.200.47	Indicates the device's IP address
41	Indicates the Node ID
3968002	Indicates the Serial Number
<i>m</i>	Indicates whether backup was periodic or manual. In the example, it was manual.
82	Indicates the product type.
INI_TYPE	Indicates the type of backed-up file: INI/CONF/CLI
2258-Jan-07-2018	Indicates the time and date, formatted as: HHmm-MMM-dd-yyyy

- In the page's Backup Summary, select the device whose configuration (ini or cli script file) you want to back up on the OVOC server.
- From the Actions' drop-down, select the **Backup** option; you're prompted with a message 'Are you sure you want to upload configuration from this device?'

**Figure 4-31: Backup Manager – Backing up a Device's Configuration – Confirmation Prompt**

- Click **Upload**; the configuration is uploaded from the device to the OVOC server.

## Saving the Last Backed-up Configuration to your PC

You can save the last backed-up device configuration to your PC.

### ➤ To save the last backed-up configuration to your PC:

- In the Backup Manager page's Backup Summary, select the device whose last backed-up configuration you want to save.
- From the Actions' drop-down, select the option **Save**; the last backed-up device configuration is saved on your PC.

## Restoring the Last Backed-up Configuration to the Device

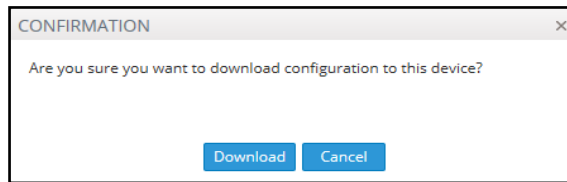
The last backed-up configuration can be restored to the device if necessary.

### ➤ To restore the last backed up configuration to the device:

- In the page's Backup Summary pane, select the device whose last backup you want to restore.

- From the Actions' drop-down, select the option **Restore Last Backup**; you're prompted with a message 'Are you sure you want to download configuration to this device?'.

**Figure 4-32: Backup Manager – Restoring a Device's Last Backup – Confirmation Prompt**



- Click **Download**; the configuration is downloaded from the PC to the device.

## Adding Links

Links are logical VoIP communication paths between devices that measure and display key metrics on calls made on them. Links are defined according to IP Group (IP network entity such as a server, e.g., IP PBX, or a group of users, e.g., LAN IP phones, with which the E-SBC communicates), Trunk Group (logical group of physical trunks and channels), Phone Number or SIP IP address.

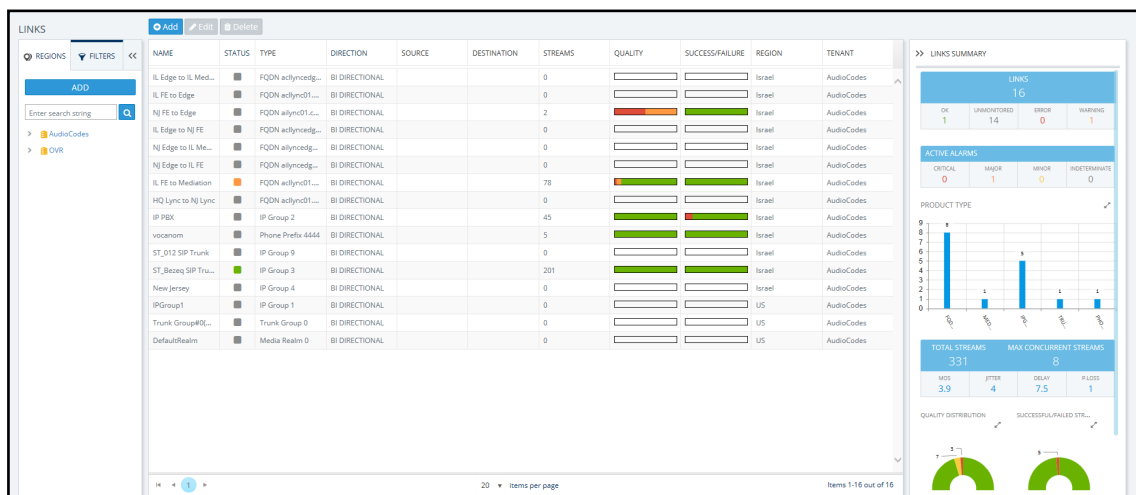
The 'source' device on which key metrics monitoring is based must be an AudioCodes device or Skype for Business device. The second device can be an AudioCodes device, Skype for Business device or a non-AudioCodes device. You can define one or more links between devices. The links are displayed in the Network Topology page. The voice quality status on each device/link is indicated by the color green, yellow or red, i.e., good, fair or poor, based on QoE thresholds described in [Obtaining Quality Statistics on Calls](#) on page 226.

You can add a link from the Topology page's **Add Link** drop-down or you can pull a line connector from a device and connect it to another device on the page.

### ➤ To add a link:

- After configuring devices, open the Links page (**Network > Links**).

**Figure 4-33: Links**



- Click **Add**.

**Figure 4-34: Link Details**

The screenshot shows a window titled "LINK DETAILS" with a close button (X) in the top right corner. Inside the window, there are five labeled input fields on the left and their corresponding controls on the right:

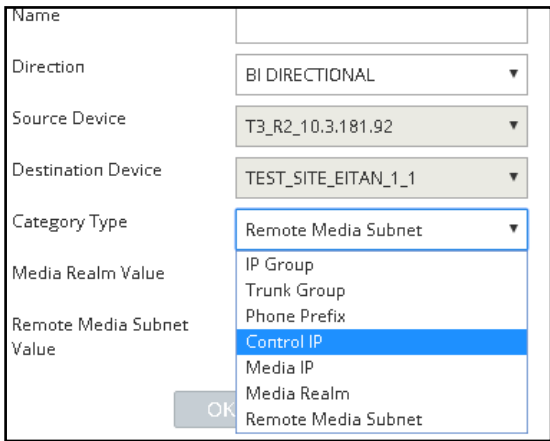
- Name \***: A text input field.
- Direction**: A dropdown menu with "BI DIRECTIONAL" selected.
- Source Device \***: A dropdown menu.
- Destination Device \***: A dropdown menu.
- Category Type \***: A dropdown menu with "Media Server" selected.

At the bottom of the window, there are two blue buttons: "OK" and "Close".

3. Use the following table as reference.

**Table 4-8: Adding a Link – Parameter Descriptions**

Parameter	Description
Name	Enter an intuitive name for the link to facilitate effective management later.
Direction	Defines the direction of the port link between source and destination device. When the link is configured as <b>Bi Directional</b> (for example), a bi-directional port will be used for this connection.
Source Device	From the drop-down list, select the source device <i>from which</i> to link to the destination device. You can alternatively search for it.
Destination Device	From the drop-down list, select the destination device <i>to which</i> to link from the source device. You can alternatively search for it.
The link counts and computes statistics on all calls that originate in the source device, based on one of the following Category Types (selected from the 'Category Type' drop-down:	
Category Type	From the drop-down select one of the following Category Types. Based on your selection, the link will count and compute statistics on all calls originating in the source device.

Parameter	Description
	
	IP Group - Defines the source device IP-Group index (a list of options may be available).
	Trunk Group - Lets you configure Trunk Groups, i.e., logical groups of physical trunks and channels each of which can include multiple trunks and ranges of channels. Trunk Groups need to be configured and assigned with telephone numbers to enable and activate the channels of the device. After configuring Trunk Groups, you need to use them for routing incoming IP calls to the Tel side, which is represented by a specific Trunk Group (ID). You can also use Trunk Groups for routing Tel calls to the IP side.
	Phone Prefix - Defines the prefix text of a phone number or SIP URI string. See the Note following for more information.
	Control IP - Defines a valid IP-Address on which SIP control messages are originated.
	Media IP - Defines a valid IP-Address on which SIP media messages (voice/fax) are originated. See the Note following for more information.
	Media Realm - Defines the source device Media Realm index (a list of options may be available).
	Remote Media Subnet - Defines the source device Media Realm subnet index (a list of options may be available; Media Realm must also be defined).
	FQDN - Available only when the source device is a Skype for Business device. The FQDN of the selected source and destination devices.

4. The field below 'Category Type' (see the preceding parameter) is the *category value* field which updates according to what you selected for 'Category Type'. If for 'Category Type' you selected:

- **IP Group** (for example), then **IP Group Value** is displayed in this field. Enter the IP Group's ID.

- **Trunk Group** (for example), then **Trunk Group Value** is displayed. Enter the Trunk Group's ID.
- **Control IP** (for example), then **Control IP Value** is displayed. Enter the IP address (the actual IP address, not the group ID).
- **Media IP** (for example), then **Media IP Value** is displayed. Enter the IP address (the actual IP address, not the group ID).

Note that some categories for 'Category Type', like **Remote Media Subnet** and **FQDN**, present two value fields, as shown in the following figure.

The image shows a 'LINK DETAILS' dialog box with the following fields:

- Name:** A text input field.
- Direction:** A dropdown menu with 'BI DIRECTIONAL' selected.
- Source Device:** A dropdown menu with 'T3\_R2\_10.3.181.92' selected.
- Destination Device:** A dropdown menu with 'TEST\_SITE\_EITAN\_1\_1' selected.
- Category Type:** A dropdown menu with 'Remote Media Subnet' selected.
- Media Realm Value:** A dropdown menu with 'DefaultRealm #0' selected.
- Remote Media Subnet Value:** A text input field.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.



If you configured parameter 'Category Type' as **Phone Prefix**, **Control IP** or **Media IP** (see the previous parameter), you can enter a *regular expression* instead of a string in the field under 'Category Type' which updates according to 'Category Type'. If the regular expression will be matched, the call will be sent over the link. Following are examples of regular expressions:

. \* = any value will be accepted, for example, abc, 123, abc123

a.\* = any value beginning with the letter 'a' will be accepted, for example, abc, a, abc123

.\*a = any value ending with the letter 'a' will be accepted, for example, bca, a, bc123a

\\d = any value containing a single digit will be accepted, for example, 1, 2

\\d\\d\\d\\.\\d\\d\\.\\d\\d\\.\\d\\d = any value that contains (three digits - point - two digits - point - three digits - point - three digits) will be accepted, for example, IP address **172.17.118.165**

To test complex regular expressions use either:

<https://www.freeformatter.com/regex-tester.html>

-OR-

<https://regex101.com/>

5. Click **Apply**; the link is added and displayed in the SEM.



- Statistics obtained from **Links** form a *subset* of those obtained from **Devices**
- Links statistics are obtained from *streams*. A **stream** is a single leg of an SBC call. It's therefore possible for the total links streams statistics to be higher than the total devices calls statistics. For example, when a call is sent from IP Group 1 to IP Group 2 on same device, and there are two links configured to aggregate streams from IP Group 1 and IP Group 2 respectively, the total **Links** statistics will present it as *twostreams* but **Devices** statistics will present it as *one call*.
- Links** are *logical* entities. Multiple links defined on the same device may therefore aggregate statistics on the same streams, so the total number of **links** streams statistics in the network may be higher than the total number of actual streams statistics in the network.

It's therefore recommended to avoid overlapping links definitions.

## Adding Sites

A site is a group of endpoints under which endpoints (phones) are located. You need to define a site under a region. The region must be defined under a tenant.

### ➤ To add a site:

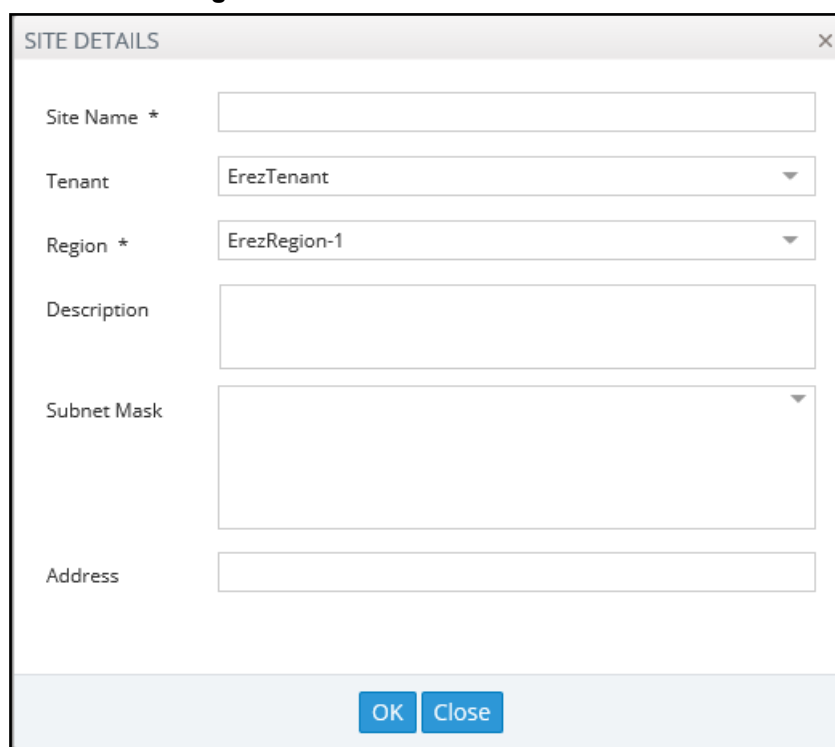
- After configuring the region under which to locate the site, open the Sites page (**Network > Sites**).

Figure 4-35: Sites

NAME	STATUS	ENDPOINTS	QOE STATUS	CALLS	MAX CONCUR...	QUALITY	SUCCESSFUL/FAIL	MANAGEMENT...	REGION	TENANT
AutoDetection	<span style="color: orange;">■</span>	140	<span style="color: gray;">■</span>	0	0			<span style="color: orange;">■</span>	AutoDetection	AudioCodes
AutoDetection	<span style="color: orange;">■</span>	77	<span style="color: gray;">■</span>	0	0			<span style="color: orange;">■</span>	AutoDetection	OVR

- Click **Add**.

Figure 4-36: Site Details



The screenshot shows a 'SITE DETAILS' dialog box with the following fields:

- Site Name \* (text input)
- Tenant (dropdown menu, currently showing 'ErezTenant')
- Region \* (dropdown menu, currently showing 'ErezRegion-1')
- Description (text input)
- Subnet Mask (dropdown menu)
- Address (text input)

At the bottom of the dialog are 'OK' and 'Close' buttons.

3. From the 'Region' drop-down, select the region under which to locate the site.
4. Provide an intuitive name for the site to facilitate effective, intuitive management later.
5. Enter a description of the site to facilitate effective, intuitive management later.
6. Enter a Subnet Mask or multiple Subnet Masks. The format must be (for example) 255.255.0.0/1. Used for auto detection of endpoints. Must be contained in the same subnet mask as the subnet mask of the region under which it is defined - if the region was configured with a subnet mask.
7. [Optional] In the 'Location' field, enter the first letters in the name of the city / country in which to locate the site, and then select the city / country from the list that pops up.
8. Click the now-enabled **OK** button; the site is added.

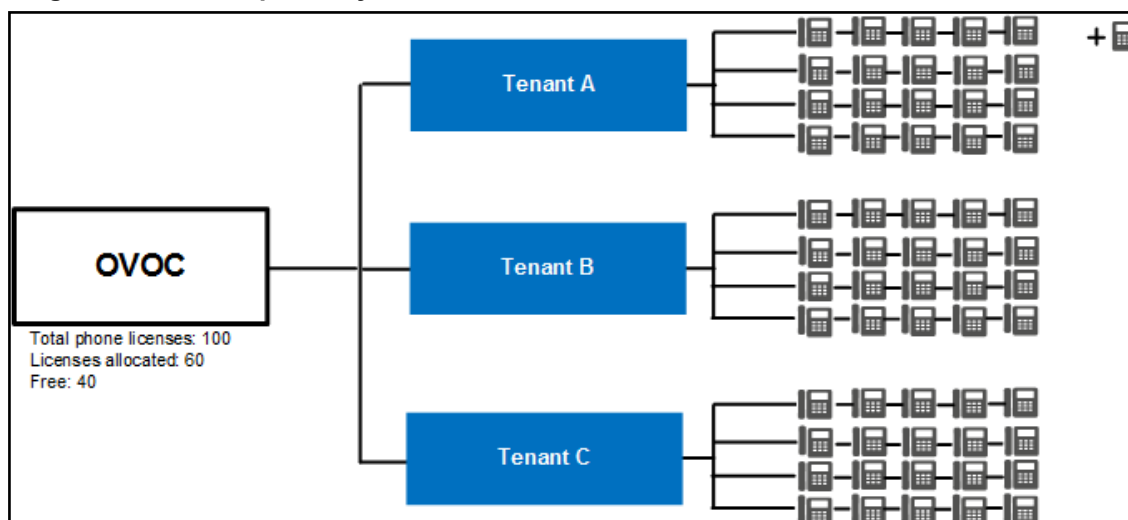
## Managing Endpoints

The OVOC supports endpoints management through the directly accessible Device Manager application.

## Dynamic Allocation of Endpoint Licenses

The OVOC *dynamically allocates* endpoint licenses to tenants by default, so that distribution is evenly and effectively performed. When a phone (endpoint) is connected to the network for the first time, it reports to the OVOC with a keepalive message. The OVOC adds the phone to its database and dynamically allocates licenses to its tenant.

Here's an example to clarify the principle of dynamic allocation.

**Figure 4-37: Example of Dynamic Allocation of Phone Licenses to Tenants**

In the example (refer to the figure above):

- Out of the total number of phone licenses which the enterprise purchased (100), indicated by OVOC server parameter 'Managed Endpoints', the OVOC has already allocated 60.
  - Tenant A was allocated 20
  - Tenant B was allocated 20
  - Tenant C was allocated 20
- The OVOC is left with 40 free phone licenses which it can still allocate to tenants (100 total – 60 allocated = 40 free)
- A new phone is connected to the enterprise network
- The OVOC detects the new phone added under Tenant A, adds the phone to the OVOC database and dynamically allocates to the phone's tenant 5% of the number of phone licenses that can still be allocated (5% of 40) or, if this results in less than 5 licenses, then 5 are allocated. 5% of 40 is 2, so in the example, 5 licenses are allocated to Tenant A.



- Applies to all AudioCodes phones whose management is supported by Device Manager, and to all phones which support SIP PUBLISH protocol and whose QoE management is supported by the OVOC's Reports application.
- Before version 7.4.2000, if a tenant's allocation was full, the OVOC dropped the phone and the user manually added it to another tenant in the OVOC GUI.
- An alarm *endpointsFloatingLicenseEvent* is sent when dynamic allocation occurs. See the *Alarms Guide* for more information.

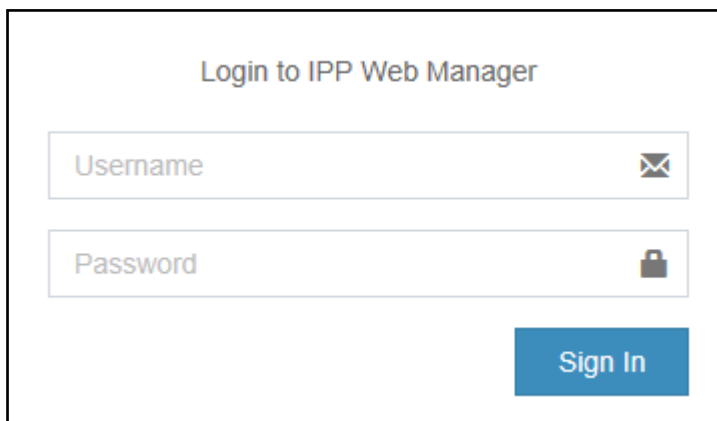
## Configuring Endpoints

The OVOC lets you directly access the Device Manager application to configure endpoints (phones).

### ➤ To access the Device Manager:

1. Select **Configuration** from the Endpoints drop-down under the Network menu.

Figure 4-38: Login to Device Manager



Login to IPP Web Manager

Username

✉

Password

🔒

Sign In

2. See the *Device Manager Administrator's Manual* for detailed information on how to configure phones.

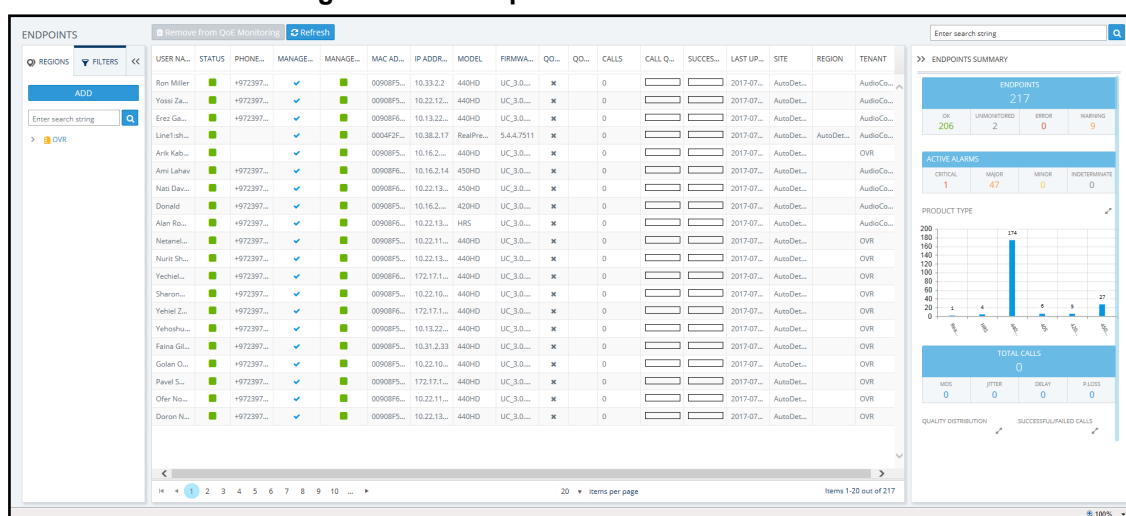
## Monitoring Endpoints Status

The OVOC lets you monitor phones statuses.

### ➤ To monitor phones statuses:

1. Open the Endpoints page (**Network > Endpoints** drop-down > **Status**).

Figure 4-39: Endpoints - Status



2. See the *Device Manager Administrator's Manual* for detailed information on how to determine phones statuses.

## Removing Endpoints from QoE Support

Removing an endpoint from QoE monitoring removes the endpoint from QoE support, freeing the used license. It does not remove the endpoint from display in the Endpoints page of the OVOC.

### ➤ To remove an endpoint from QoE support:

1. Open the Endpoints page as described previously and select the phone to remove from QoE support.
2. Click the button **Remove from QoE Monitoring**; the relevant 'QoE Supported' column is updated with **X** instead of **✓**.

## 5 Managing SBC Licenses

SBC licenses can be managed using one of following three optional methods:

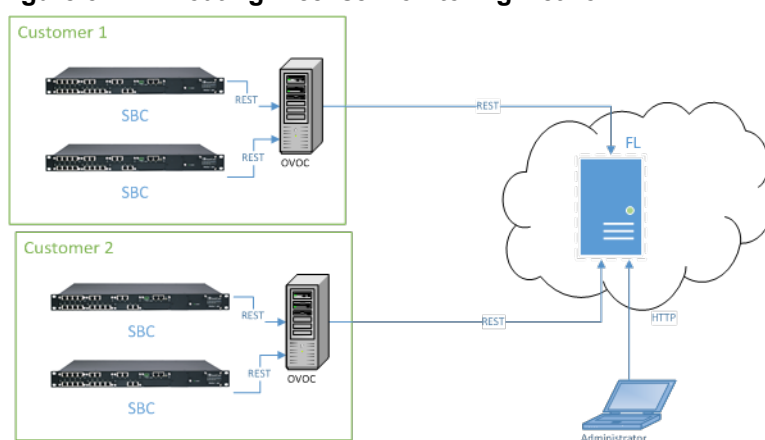
- **Floating License monitoring method** (see [here](#))
  - This method replaced the legacy method of using the OVOC Advanced Monitoring package (SEM)
  - The method requires the SBCs to be loaded with version 7.2.202 or later and an OVOC version 7.2.3000 or later
- **Fixed License Pool** (see [Managing Device Licenses in the Fixed License Pool](#) on page 134)
  - Best when multiple SBCs are deployed and management wants to *centrally manage* the licenses of all
  - Allows a 'tenant' operator to update licenses from a central pool in a simple process
- **Locally** by loading an ini file to the device using the Web interface, without requiring the OVOC. See the device's *User Manual*.

### Configuring SBC Floating License Monitoring

Floating License monitoring can be configured on the AudioCodes SBCs and OVOC. For more information, see also the *Mediant SBC User's Manual*.

The Floating License monitoring method replaced the legacy method of using the OVOC Advanced Monitoring package (SEM). The Floating License method requires that the SBCs are loaded with version 7.2.202 or later and an OVOC version 7.2.3000 or later.

**Figure 5-1: Floating License Monitoring Network**



Here's how the Floating License method works:

- SBCs report their usage statistics at short intervals (typically every 5 minutes) to the OVOC.
- The OVOC accumulates these reports and sends them once a day to the AudioCodes Floating License server. Since all communications occur over HTTPS, a special firewall setup is unnecessary in most cases.



Important note before installation: To set up floating license monitoring for a new customer, a floating license account must be created on the AudioCodes cloud license manager (CLM) service. The CLM account is created by AudioCodes within a few days of receiving a floating license order and signing of the floating license's Terms and Conditions. After the account is set up and ready for use, a confirmation email is sent to the email address used to receive the customer's OVOC product key. Make sure the confirmation email is received before attempting to connect OVOC to the CLM service. If no confirmation email is received, contact your AudioCodes representative and provide your OVOC product key to verify the CLM account was set up.

Managed as an AudioCodes cloud service, the Floating License feature is a network-wide license intended for customer deployments featuring multiple SBCs sharing a dynamic pool of resources. The feature simplifies network capacity planning and delivers cost benefits related to aggregated call statistics, follow-the-sun scenarios and disaster recovery setups that involve two or more data centers.

The feature allows customers to 'pay as they grow' by eliminating the need to manually purchase additional SBC licenses when capacity requirements increase. Customers initially purchase license capacity based on estimated requirements but may later experience business growth and therefore require increased session capacity. In this case, customers are billed for the additional sessions. SBCs deployed in the network are 'open' to maximum hardware capacity utilization based on predefined profiles. SBCs can alternatively be configured by operators with customized session capacity profiles.

## Configuring the OVOC for Floating License Monitoring

Configuration should only be performed once for the OVOC of each customer.

### ➤ To configure the OVOC:

1. Add a new OVOC operator of type 'System' dedicated to the Floating License (i.e., 'Floating License\_User').
  - They must have Admin or Operator security level
  - Password expiration must be set to never expire
  - SBCs use them to communicate with the OVOC for the floating license reports
2. Make sure the OVOC is configured with a Feature Key which enables Floating License.
  - Open the License Configuration page (**System > Administration > License > Configuration**).
  - Make sure that 'Status' under the page section Floating License, is **Enable**.

**Figure 5-2: Floating License Status - Enable**

LICENSE CONFIGURATION		Load License	
ADMINISTRATION << ▲ LICENSE Configuration Tenants Allocations Floating License	GENERAL		FLOATING LICENSE
	Machine ID:	18AC268AB262	Status: Enable
	Product Key:	UAAC6E671FF02XH6	SBC Sessions: 0
	Status:	Enable	SBC Registrations: 0
	Reason:		SBC Transcoding: 0
	Expiration Date:	01-01-2037	SBC Signalling: 0
	Expiration Days Left:	6373	

3. Open the Floating License page (**System > Administration > License > Floating License**).

**Figure 5-3: Floating License**

4. Configure the parameters like this:

- **Floating License OVOC Operator:** Use the new operator you configured [here](#).
- **Floating License Server Address:** Set to: **clm.audiocodes.com**
- **Change Floating License Key:** Set to the OVOC Product Key. To find out the OVOC Product Key, view the string in the License Configuration screen (**System > Administration > License > Configuration**) under section 'General'.

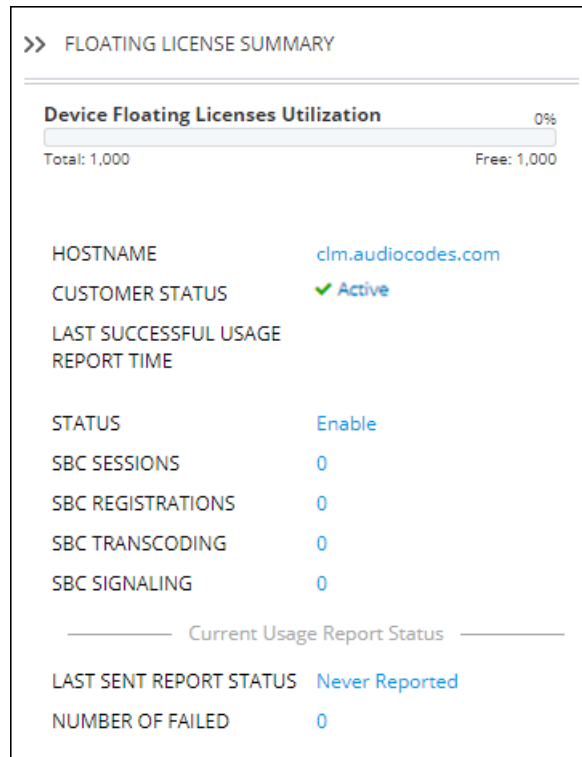
**Figure 5-4: Product Key**

5. Open the Device Floating License page (**Network > Devices > Floating License**).

**Figure 5-5: Device Floating License Page**

NAME	PRODUCT TYPE	IP ADDRESS	HA	MANAGED	LAST REPORT TIME	FLOATING LICENSE STATUS	DEVICE STATUS	CONNECTION LOST TIME	CONFIG STATUS	REPORT STATUS	REGION	TENANT
SBC 10.36.49.1	SW SBC	10.36.49.1	*	✓		Active	Online		Green	Red	EresRegion	EresTenantz

- Make sure in the Device Floating License page that the OVOC successfully registered with the Floating License. Make sure that 'Customer Status' in the device's Floating License Summary pane displays **Active**.

**Figure 5-6: Customer Status**

## Adding an SBC to the Floating License

Before adding an SBC to the Floating License, add an SBC to the OVOC using one of these options:

- Auto device detection. This is the Automatic Provisioning a.k.a. Zero Touch feature. See [Enabling Initial Connection Provisioning](#) on page 102 for more information.
- Manually from the AC Device page (**Network > Add > AC Device**).
- Using the SBC's Web interface.



The Floating License method does not require configuring an open license on the SBC (obtained via ordering of one of the device float CPNs i.e. SW/M500/FLOAT). The SBC is authorized by the OVOC to operate in a mode with no resource restrictions.

### ➤ To add an SBC to the Floating License:

1. Open the Floating License page (**Setup menu > Administration tab > Maintenance folder > Floating License**).
2. From the 'Floating License' drop-down list, select **Enable**.

**Figure 5-7: Enable Floating License**

GENERAL

Floating License Enable ⚡

Connection with OVOC Connected to OVOC 🟢

OVOC IP Address 172.17.140.203

OVOC Product Key 3F1927F8DF64

3. Reset the device with a burn-to-flash for your settings to take effect. After the device resets, it connects with OVOC and the following read-only fields display OVOC-related information:
  - 'Connection with OVOC': Displays the device's connectivity status with OVOC:
    - ◆ "Connected to OVOC": The device is connected to OVOC.
    - ◆ "Disconnected from OVOC" The device is temporarily disconnected from OVOC due to problems with the network (HTTPS TCP connection).
    - ◆ "Not Connected to OVOC": The device is not connected to OVOC.
  - 'OVOC IP Address': Displays the IP address of OVOC.
  - 'OVOC Product Key': Displays the **Product Key of the OVOC tool that is providing the Floating License**.
4. From the 'Allocation Profile' drop-down list, select an SBC license Allocation Profile. The Allocation Profile determines the capacity of each SBC license type that you want allocated to your device by OVOC. You can choose from factory default profiles, which may suit your deployment requirements or you can configure your own customized profile. The optional factory default profiles include:
  - **SIP Trunking**: This profile is suited for SIP Trunking applications (i.e., where user registration is typically not required)
  - **Registered Users**: This profile is suited for applications where user registration is required.

To configure your own profile, select **Custom**, and then configure the capacity for each SBC license type in the corresponding 'Allocation' field. When you hover your mouse over each field, a pop-up appears displaying the maximum capacity that can be supported by the device.

**Figure 5-8: Maximum Capacity for Each SBC License Type**

Allocation Profile	Custom	
	Allocation	Limit
Far End Users	1600	<input type="text"/>
SBC Media Sessions	400	<input type="text"/>
SBC Signaling Sessions	400	<input type="text"/>
Transcoding Sessions	60	<input type="text"/>



When configuring your own customized profile (i.e., using the **Custom** option), the Transcoding Session capacity license cannot be changed in the 'Allocation' field, but you can reduce the license using its corresponding 'Limit' field.

- Explanation of each profile:
  - ◆ Far End Users (FEU) (# of concurrent users that can be registered on the device)
  - ◆ SBC Sessions (# of concurrent SBC call sessions-media and signaling)
  - ◆ SBC Signaling Sessions (# of concurrent SIP messages- only signaling)
  - ◆ Transcoding Sessions (# of concurrent codec types)
- 5. Reset the device with a burn-to-flash for your settings to take effect.
- 6. Once you have configured the Allocation Profile, you can modify each SBC license capacity without resetting the device. To do this, select the check box corresponding to the license type you want to modify, and then in the corresponding 'Limit' field, enter a new value, and then click **Apply**.

- Open the OVOC's Device Floating License page (**Network > Devices > Floating License**) and verify that the newly added SBC appears in the list and that the last report time is updated (indicating that the SBC has successfully sent a report to the OVOC). As reports are sent every 5 minutes, this may take up to 5 minutes to show.

**Figure 5-9: Device Floating License Page – Newly Added SBC Appears in the List**

NAME	PRODUCT TYPE	ADDRESS	HA	MANAGED	LAST REPORT TIME	FLOATING LICENSE S.	DEVICE STATUS	CONFIG STATUS	REPORT STATUS	REGION	TENANT
HQ SBC	MEDIAN 2000 SBC	10.62.0.10	✓	✓	12-Jun-18 11:20:00		Green	Green	Green	Israel	A
NY SBC	MEDIAN 1000 PRO	172.28.1.3	✗	✓	12-Jun-18 11:20:00		Green	Green	Green	US	A

- Use the following table as reference to the page's columns.

**Table 5-1: Floating License Page Column Descriptions**

Column	Description	
Name	Indicates the name of the managed device	
Product Type	Indicates the SBC device type.	
Address	Indicates the IP address of the managed device.	
HA	Indicates the HA status of the device.	
Managed	Indicates whether the device is managed by the Floating License service server.	
Last Report	Indicates the date and time that the last usage report was sent from the OVOC to the Floating License service server.	
Floating License Status	Indicates the global device status reflecting the Device Status, Config Status and Report Status states.	
	Green	<b>OK:</b> Device Status, Config Status and Report Status are green.
	Red	<b>Error or Config Error:</b> Indicates Device Status, Config Status or Report Status errors (red).
	Grey	<b>Unmanaged:</b> Device is unmanaged by OVOC <b>Unmonitored:</b> Device is unmonitored by OVOC

Column	Description	
Device Status	Green	<b>Connected:</b> Device is successfully connected to the Floating License OVOC service.
	Red	<p><b>Rejected:</b> Device Floating License has been revoked by the Cloud Floating License service and as a result the device's CAC is reset to 0.</p> <p><b>Not Connected:</b> Device is unable to establish a connection with the Floating License OVOC service (CAC 0)</p> <p><b>Temporarily Disconnected:</b> Device is temporarily disconnected from the Floating License OVOC service due to problems with the HTTPS TCP connection.</p>
	Grey	<p><b>Unmanaged:</b> The device is currently not managed by the OVOC Floating License service.</p> <p><b>Unmonitored:</b> The device is currently unmonitored by the OVOC Floating License service.</p> <p><b>Not Applicable:</b> The device was loaded with the Floating License feature disabled. The operator must enable the feature on the SBC device and reset it.</p>
Config Status	Green	<b>Success:</b> Indicates that the device's SNMP configuration is successfully updated.
	Red	<b>Failure:</b> Indicates that the device's SNMP configuration has not been updated successfully. For example, the Floating License REST operator's user password or username has not been updated correctly.
	Grey	<p><b>Not applicable:</b> Indicates that the device was added to the OVOC but is not yet managed.</p> <p><b>Unmonitored:</b> Indicates that the device is currently unmonitored by OVOC.</p>
Report Status	Green	<b>OK:</b> Indicates that a report was successfully sent from the device to the OVOC for the last reporting interval.
	Red	<b>Fail:</b> Indicates that there was a reporting failure for the last reporting interval.
	Grey	<b>Unmonitored:</b> Indicates that the device is currently unmonitored by OVOC.
Region	Indicates the device's region.	
Tenant	Indicates the device's tenant.	

- Click the **Actions** button. See [here](#) for information about the actions that you can perform in the Device Floating License page.

## Performing Floating License Actions

Here're the Actions you can perform in the Device Floating License page:

- Unmanage (see [here](#))
- Update (see [here](#))

- Reset (see [Reset](#) below)
- Register (see [Register](#) below)

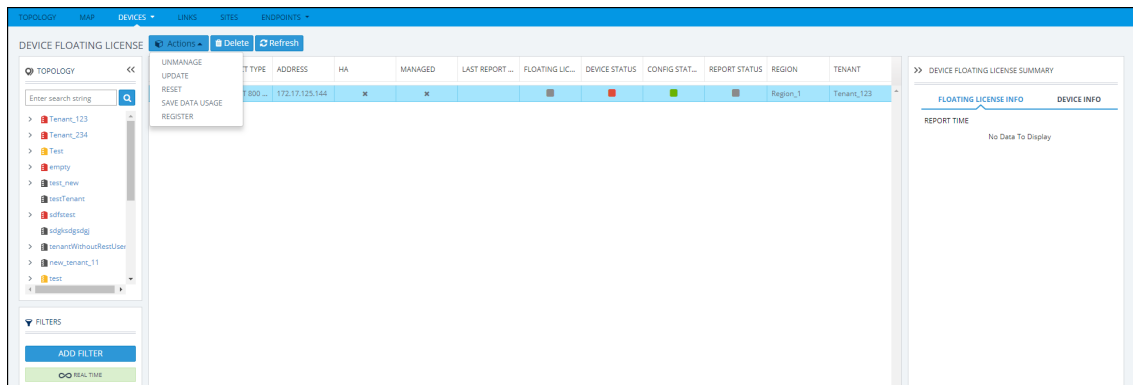
## Unmanage

This Action allows the device to be unmanaged by the Floating License method.

### ➤ To allow the device to be unmanaged by the Floating License method:

- In the Device Floating License page, select the SBC to unmanage and then from the Actions drop-down menu, select **Unmanage**.

**Figure 5-10: Device Floating License Page – Unmanage Action**



## Update

Select this menu option for the action to update the HTTPS Rest connection between the device and OVOC.

## Reset

Select this menu option when:

- The SBC is connected to the OVOC and Floating License is enabled.
- One of the following SBC Web interface Floating License parameters is updated on the device:
  - Allocation Profile
  - Allocation Signaling Sessions
  - Allocation Media Sessions
  - Allocation Registered Users
- A 'Limit' value is configured for one of the above SBC Web interface Floating License parameters.
- The SBC's ini file parameter 'SoftwareDSP' is updated (only applies to Mediant 9000, Mediant SE and Mediant VE).

## Register

Select this menu option for the action to perform random registration to the Floating License Cloud service for the device.

## Configuring OVOC-Floating License Service Communications

SBCs are connected to the OVOC over SNMP. Floating License service functions are managed over TCP/HTTPS REST connections. For more information, see the *OVOC IOM* and the *OVOC Security Guidelines*.

➤ **To configure device Floating License parameters for OVOC-Floating License communications:**

1. Open the Floating License page (**System > Administration > License > Floating License**).

**Figure 5-11: Floating License**

2. Configure the parameters using the following table as reference.

**Table 5-2: Device Floating License Configuration Parameter Descriptions**

Parameter	Description
Floating License OVOC Operator	Specifies the OVOC operator with REST authorization to receive and respond to REST requests from the SBC devices. This operator must be a 'System' type operator with either 'Admin' or 'Operator' security permissions.
Floating License Server Address	Specifies the server address of the Floating License Service platform: <b>CLM.audiocodes.com</b> (default)
Change Floating License Key	Enter the AudioCodes provided OVOC Product Key string used to authenticate the connection between the OVOC and the Floating License Service. You can view this string in the License Summary screen ( <b>System &gt; Administration &gt; License &gt; Summary</b> ).

## Viewing Floating License Summaries

The OVOC's Device Floating License page displays summary panes on the right side of the page. Panes you can view are:

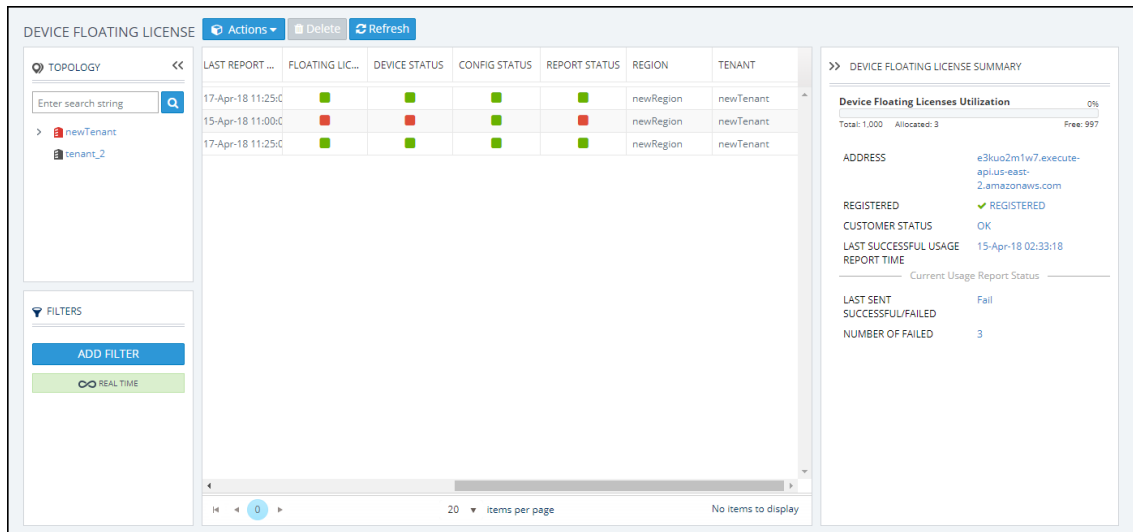
- Device Floating License Utilization pane (see [here](#))
- Floating License Info pane (see [Viewing Floating License Info](#) on page 132)
- Device Info pane (see [Viewing Device Info](#) on page 132)

## Device Floating License Utilization Pane

This pane is only displayed when no device is selected in the page.

➤ **To view the pane if a device is selected:**

1. Press the **Ctrl** key and then click the entry on the page that is selected.

**Figure 5-12: Device Floating License Summary**

2. Use the following table as reference to the pane.

**Table 5-3: Device Floating License Utilization Pane Description**

License Utilization	Description
Total/Allocated bar	Indicates the percentage of SBC devices in this OVOC installation that are managed by the Floating license. For example, if the customer has purchased licenses for 100 devices and 50 are currently managed, then this bar displays 50 allocated devices and 50 free devices.
Address	Indicates the IP address or FQDN of Floating License Service.
Registered	Indicates whether OVOC is successfully registered to Floating License Service.
Customer Status	Indicates the state of the connection with the Floating License service. <b>OK</b> - Indicates that a successful connection with the Floating License has been established. <b>Blocked</b> - Customer account has been blocked by the Floating License Service. <b>Unknown</b> - Status is undetermined by the OVOC
Last Successful Usage Report Time	Indicates the time and date of the last successful usage report update that was sent from OVOC to the Floating License Cloud service.
Last Sent Successful/Failed	Indicates whether the last attempt to send a usage report to the Floating License Cloud service was successful.
Number of Failed	Indicates the number of failed attempts to send usage reports to the Floating License Cloud service

## Viewing Floating License Info

The OVOC's Device Floating License page displays the 'Floating License Info' summary pane only when a device is selected in the page.

### ➤ To view the pane:

1. Select an entry on the page.

**Figure 5-13: Device Floating License Summary – Floating License Info**

Report Time	Current	Max Config	Max Actual
Media Se...	0	5000	5000
Registrat...	0	500	500
Signaling...	0	5000	5000

2. Use the following table as reference to the pane's session capacities displayed.

**Table 5-4: Device Floating License Summary - Floating License Info**

Session Capacity	Description
Current	Indicates the currently utilized session capacity of the SBC device.
Maximum Configuration	Indicates the customer configured session capacity on the SBC device.
Maximum Actual	Indicates the maximum physical session capacity of the SBC device.

## Viewing Device Info

The OVOC's Device Floating License page displays the 'Floating License Info' summary pane only when a device is selected in the page.

### ➤ To view the pane:

1. Select an entry on the page if none is selected and then in the Device Floating License Summary pane, click the **Device Info** tab.

**Figure 5-14: Device Floating License Summary – Device Info**

NAME	172.17.125.79
PRODUCT TYPE	SW SBC
ADDRESS	172.17.125.79
HA	✗ No
MANAGED	✓ Yes
FLOATING LICENSE STATUS	✗ Error
DEVICE STATUS	✗ Not Connected
CONFIG STATUS	✓ Success
REPORT STATUS	✗ Fail
REGION	newRegion
TENANT	newTenant

2. The pane summarizes the columns displayed in the main section of the Device Floating License page.

## Saving a Usage Data Report to your PC

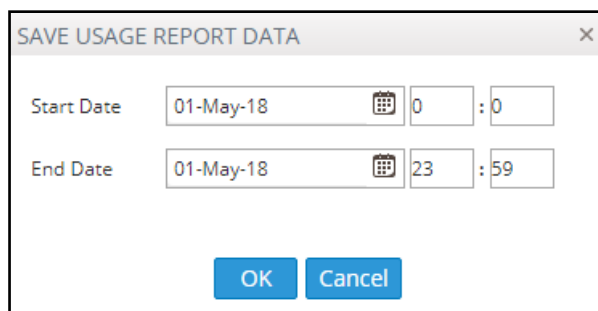
Customers who do not want usage reports to be sent *automatically* to AudioCodes but would rather export reports to a CSV file, download to a PC and then send *manually* to AudioCodes, can benefit from this feature.

If you do not use this feature, the SBC automatically sends usage reports every five minutes to the OVOC. Each report includes the currently configured license session values and the device's HA state.

### ➤ To manually export a usage report to a CSV file:

1. Open the Device Floating License page (**Network > Devices > Floating License**) and click **Save Data Usage**.

**Figure 5-15: Save Usage Report Data**



SAVE USAGE REPORT DATA

Start Date 01-May-18 0 : 0

End Date 01-May-18 23 : 59

OK Cancel

2. In the Save Usage Report Data screen shown above, define the period on which to produce the usage report data and then click **OK**.

## Managing Device Licenses in the Fixed License Pool



Only a 'tenant' operator can manage the Fixed License Pool. To configure a 'tenant' operator, see [License Pool Operator](#) on page 86 for more information.

Customers who deploy multiple SBCs and want to *centrally manage* the licenses of all SBCs deployed will benefit best from the Fixed License Pool feature. This feature allows updating a device's license using the process shown here:



- OVOC operator updates SBC license in OVOC's License Pool
- OVOC notifies SBC that the License Pool has been updated
- SBC requests updated license from OVOC
- OVOC sends the updated license to SBC
- SBC polls OVOC for license updates
  - every 12 hours
  - when the SBC is reset
  - (HA) when switchover and synchronization by the new active device are performed
- OVOC sends the license update to the SBC (if an update is discovered)



An SBC's license is valid for seven days but this is reset each time a successful connection is established between it and the OVOC License Pool. If the SBC cannot connect to the License Pool for seven days, its license expires and resets with its initial 'local' license. This feature prevents misuse of issued licenses.

The Fixed License Pool page in the OVOC allows you to:

- centrally distribute session licenses to multiple devices according to capacity requirements
- manage the licenses of multiple devices without changing their local License Key.
- add/remove licenses to/from devices according to site requirements, independently of AudioCodes.
- apply different settings to each device without requiring a new License Key file per device from AudioCodes each time.
- manage licenses for multiple enterprise customers [ITSPs].

The Fixed License Pool supports the following license types:

- SBC sessions (includes both media and signaling)
- SBC Registrations (also referred to as Far-End Users)
- SBC Signaling sessions (includes only signaling)
- Transcoding sessions

The customer purchases a bulk number of licenses of these types and obtains a License Key to install on the OVOC. The customer can then:

- allocate licenses to any SBC managed by the OVOC
- move licenses from any SBC back to the License Pool
- move licenses from one SBC to another
- purchase additional licenses for the pool at any time

When license capacity is fully utilized, the SBC rejects calls. If the SBC also has a 'local' license, the two are cumulated to constitute a single license.

➤ **To update a license using the Fixed License Pool:**

1. Open the Fixed License Pool page (**Network > Devices**).
2. In the page, select a device and then click the **Actions** button.

**Figure 5-16: Fixed License Pool - Refresh Device License**

IP ADDRESS	HA	LP STATUS	LAST REQUEST TIME	REGION	TENANT
10.8.50.18			11-Oct-18 11:16:04	region2	tt
10.21.50.20 CB			16-Sep-18 00:46:17	Region1_Elshvea	Elshvea
mm_5.9.3.3				region2	tt
10.8.12.30			02-Oct-18 11:38:52	Region1_Elshvea	Elshvea
10.8.50.15				Region1_Elshvea	Elshvea
10.8.50.17				Region1_Elshvea	Elshvea
10.21.50.41-1564981...				AutoDetection	Elshvea
181.1				Region1_Elshvea	Elshvea
10.3.3.201				Region1_Elshvea	Elshvea
10.36.41.1				fgdddf	mimic
10.36.41.2				Region1_Elshvea	Elshvea
as_1.2.1.2				Region1_Elshvea	Elshvea
test				Region1_Elshvea	Elshvea
Try				Region1_Elshvea	Elshvea
172.17.140.116				Region1_Elshvea	Elshvea
rgnag/fgds				Region1_Elshvea	Elshvea
172.17.140.76				Region1_Elshvea	Elshvea
172.17.142.76				Region1_Elshvea	Elshvea
protractor_4006281...				protractor_4006281...	protractor_4006281...
172.17.140.240				Region1_Elshvea	Elshvea
fgthgfh				Region1_Elshvea	Elshvea
10.3.181.71				Region1_Elshvea	Elshvea

3. Use the table as reference to the icons in the column 'LP Status' in the preceding figure.

**Table 5-5: LP Status**

Icon	Description
	License Pool status is OK
	License Pool status is WARNING
	License Pool status is EXPIRED
	License Pool status is CONFIGURATION ERROR
	License Pool status is FAILED
	License Pool status is OUT OF SYNC
	License Pool status is UNMANAGED
	License Pool status is APPLY NEEDED
	License Pool status is APPLY IN PROGRESS
	License Pool status is RESET NEEDED

4. From the Actions drop-down, select **Fixed License > Refresh Device License**.

## Performing License Pool Actions

The License Pool page allows operators to perform a range of actions.

### Applying a License to a Device from the Pool

You can apply a license to a device.



Applies only to HA devices. A switchover is performed to apply the license parameter on both devices.

#### ➤ To apply a license to a device:

1. In the Fixed License Pool page, from the Actions menu select **License > Apply**.

**Figure 5-17: Apply License**

The screenshot shows the 'FIXED LICENSE POOL' interface. On the left is a 'TOPOLOGY' sidebar with a search bar and a list of locations: OVR, Singapore, Voca, USA, New\_Tenat, and Devices\_Agents. The main area has a top bar with buttons: Actions (dropdown), Edit, Show, Delete, Save, and Refresh. Below this is a table with columns: MAINTENANCE, LICENSE, HIGH AVAILABILITY, EDIT, APPLY, ID, PRODUCT TYPE, IP ADDRESS, and HA. The 'LICENSE' dropdown is open, showing 'EDIT' and 'APPLY' options. The table contains several rows of device information, with the 'HA' column indicating high availability status (marked with 'x' or a checkmark).

MAINTENANCE	LICENSE	HIGH AVAILABILITY	EDIT	APPLY	ID	PRODUCT TYPE	IP ADDRESS	HA
						MEDIANT 800 CCE APPLIANCE	10.255.255.1	x
HQ SBC						MEDIANT 2600 E-SBC	10.62.0.10	✓
CCE SBC demo						UNKNOWN	172.17.247.8	x
NJ SBC						MEDIANT 1000 PRO	172.28.1.3	x
172.17.118.48-597347683						SW SBC	172.17.118.48	x
Alon MSBR						MEDIANT 500L MSBR	10.11.2.233	x
TEST device						MEDIANT 800 E-SBC	10.15.11.1	x
Marina						UNKNOWN	1.2.3.4	x
EREZ UMP Temp						User Management Pack	10.21.28.187	x

2. In the confirmation prompt, click **Apply**.

A confirmation dialog box titled 'CONFIRMATION' with a close button (X) in the top right corner. The text inside asks: 'Are you sure you want to apply runtime license on this MG?'. At the bottom, there are two buttons: 'Apply' and 'Close'.

### Saving Fixed License Pool Data to CSV File

Information displayed in the Fixed License Pool page can be exported to a CSV file. The feature is used internally when (for example) AudioCodes requires the information from a customer who has reported an issue.

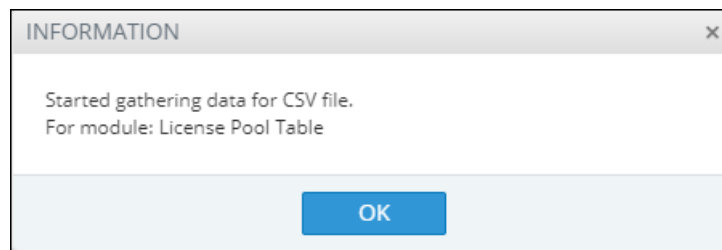
#### ➤ To export Fixed License Pool data to a CSV file:

1. Open the Fixed License Pool page (**Network > Devices > Fixed License Pool**).

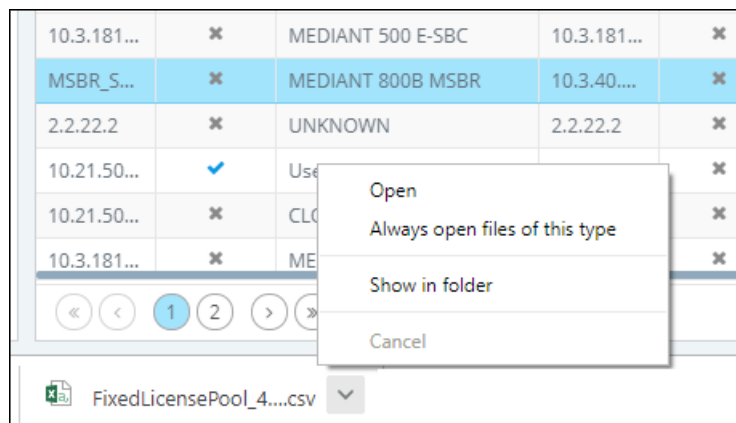
Figure 5-18: Fixed License Pool

The screenshot shows the 'FIXED LICENSE POOL' interface. On the left is a 'TOPOLOGY' sidebar with a search bar and a list of devices (Zipora2, New, Tenant12, bfd, fxc, PMS, NewPMS). Below it are 'FILTERS' and an 'ADD FILTER' button. The main area is a table with columns: NAME, MAN..., PRO..., IP AD..., HA, LP ST..., LAST..., REG..., TENA..., SBC..., SBC..., SBC..., SBC..., CB U..., CB P..., CB A..., CB VOL... The table contains multiple rows of license data. On the right is a 'DEVICE LICENSE DETAILS' sidebar with sections for 'LICENSE SUMMARY', 'LICENSE INFO', and 'DEVICE INFO'. The 'LICENSE SUMMARY' section shows 'Summary Of Tenant: Zipora2' and 'Managed Devices' with a total of 1,000 allocated and 991 free. The 'LICENSE INFO' section shows 'SBC Sessions' (1% total, 1,000 allocated, 992 free), 'SBC Signaling' (0% total, 1,000 allocated, 1,000 free), 'SBC Transcoding' (0% total, 1,000 allocated, 1,000 free), 'SBC Registrations' (0% total, 1,000 allocated, 2 free), 'Cloud Bond Allocations', 'CB Users' (0% total, 1,000 allocated, 1,000 free), and 'CB PBX Users' (0% total, 1,000 allocated, 2 free).

2. Select the device select and click **Save As**.



3. Click **OK**; locate the saved CSV file whose icon is displayed in the systray and send it to AudioCodes.
4. To open the CSV file, click its icon or right-click and select **Open**.



5. View the file opened in a CSV file editor like Microsoft's Excel.



For each license (SBC column / CB column) listed in the Fixed License Pool page, four parameters are displayed in the CSV file according to the License Info 'Pool/Local/Actual/Active'. For example, the parameters that are displayed in the CSV file for the Fixed License Pool page column 'SBC Session' are:

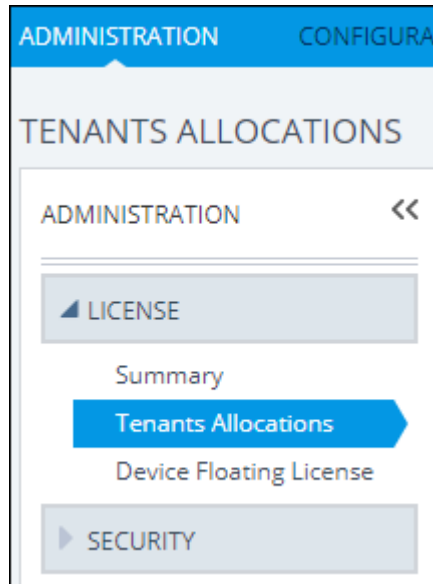
- sbcSession\_pool
- sbcSession\_local
- sbcSession\_actual
- sbcSession\_active

## Before Performing 'Manage Device' / 'Update Device'

Make sure of the following before performing 'Manage Device' or 'Update Device':

- Make sure sufficient licenses are allocated on the device's tenant (**System > Administration > License > Tenants Allocations**).

**Figure 5-19: Make Sure Sufficient Licenses are Allocated on the Device's Tenant**



- Make sure the device's tenant's 'License Pool Operator' is valid; make sure their password has not expired (**Network > Devices > Manage > select the device > Edit**).

**Figure 5-20: Make Sure License Pool Operator is Valid**

- Make sure the device is connected to the OVOC (**Network > Devices > Manage > select the device > Show**).

**Figure 5-21: Make Sure the Device is Connected to the OVOC**

DEVICE INFORMATION				
172.17.133.102-232...	AutoDetection	OK	UNLOCKED	No
NAME	REGION	STATUS	ADMIN STATE	SAVE NEEDED?
172.17.133.102	7.20A.156.009	SW SBC	232685563	No
ADDRESS	FIRMWARE	TYPE	S/N	RESET NEEDED?
<b>Management: OK</b> <b>Clear</b> <small>DEVICE ALARMS STATUS</small> <b>Unlocked</b> <small>ADMINISTRATION STATUS</small> <b>Connected</b> <small>CONNECTION STATUS</small>		<b>Voice Quality: Unmonitored</b> <b>Unmonitored</b> <small>CONTROL STATUS</small> <b>Unmonitored</b> <small>MEDIA STATUS</small> <b>Not Defined</b> <small>CONNECTION STATUS</small>		<b>License: OK</b> <b>License in Use</b> <small>MANAGEMENT STATUS</small> <b>Not Requested</b> <small>VOICE QUALITY STATUS</small> <b>OK</b> <small>LICENSE POOL STATUS</small>

## License Pool Alarms

Devices can issue the following License Pool alarms:

- acLicensePoolInfraAlarm
- acLicensePoolApplicationAlarm
- acLicensePoolOverAllocationAlarm
- acLicenseKeyHitlessUpgradeAlarm

For more information about alarms related to the License Pool, see the *OVOC Alarms Guide*.

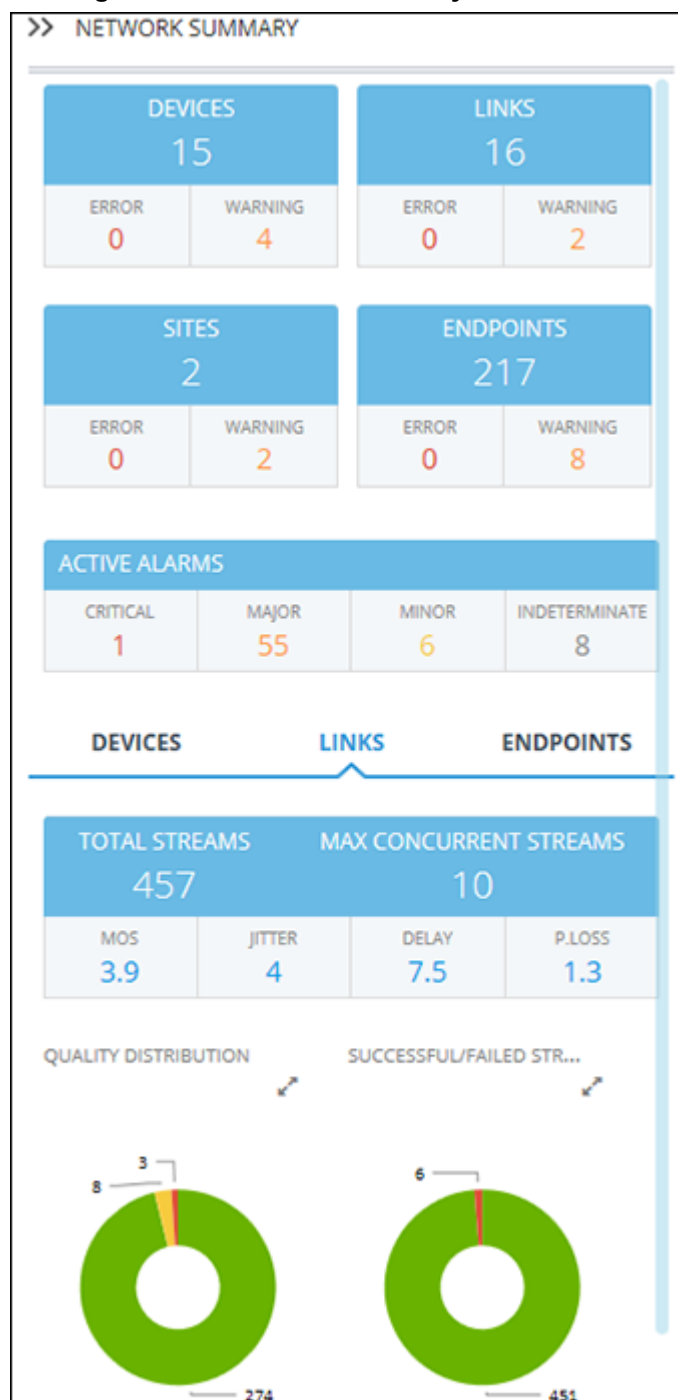
## 6 Assessing Network Health

The OVOC enables you to determine the health of your IP telephony network. The OVOC provides real-time monitoring as well as historical monitoring of network traffic, giving operators a health monitoring functionality that includes alarms and diagnostics capability.

### Assessing Health from the Network Summary

The Network Topology page displays a Network Summary pane which you can reference to quickly assess the overall health of the network.

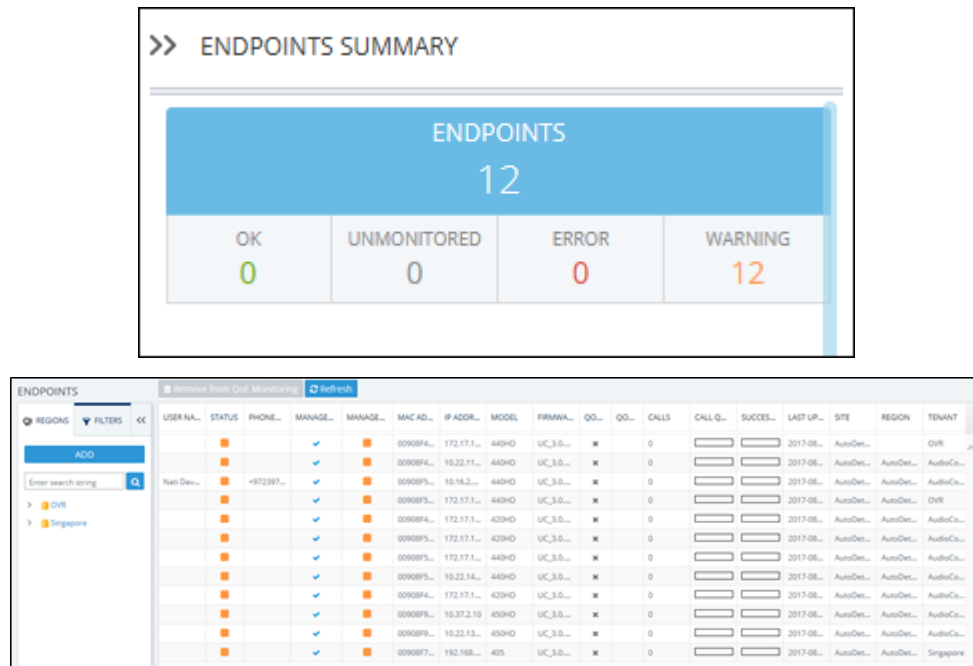
**Figure 6-1: Network Summary**



- The four upper Network Summary panes display:

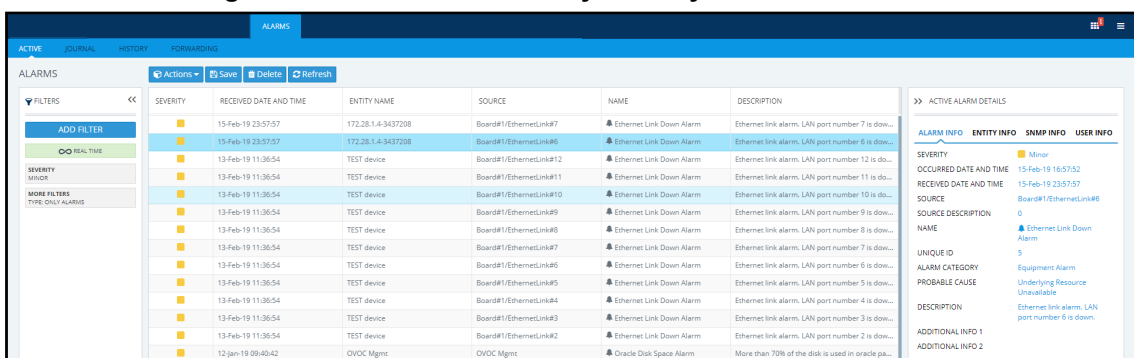
- The count of Devices, Links, Sites and Endpoints on which alarms are currently active.
- The color-coded number of Devices, Links, Sites and Endpoints whose status is currently Error / Warning. If you click the # of
  - ◆ **Devices** then the Device Management page opens displaying all devices whose status is Error / Warning
  - ◆ **Links** then the Links page opens displaying all links whose status is Error / Warning
  - ◆ **Sites** then the Sites page opens displaying all sites whose status is Error / Warning
  - ◆ **Endpoints** then the Endpoints page opens displaying all endpoints whose status is Error / Warning

Figure 6-2: Example: 12 Endpoint Warnings



- The Active Alarms pane displays:
  - The total number of Critical, Major, Minor and Indeterminate active alarms (color-coded) currently active in the network.
  - Click any severity level's total to display only alarms of that severity level in the Alarms page. Example: Under **Critical** in the Active Alarms pane above, click 1:

Figure 6-3: Alarms Filtered by Severity Level



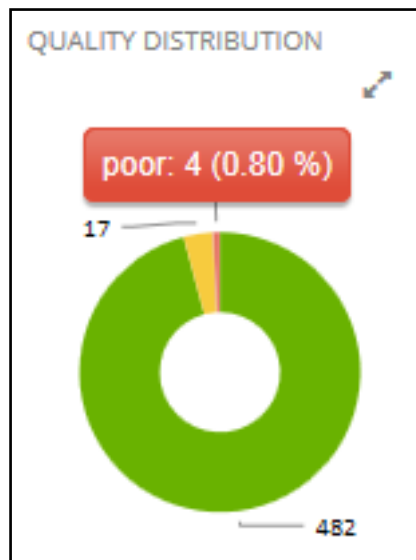
You can select an alarm in the page to view detailed information about it in the All Alarm Details pane on the right side of the page.

- In the Network Summary window, the (default) **Links** tab displays:
  - The total # of streams over links in the network.
  - The maximum # of concurrent streams over links in the network.

- The average MOS measured over links in the network.
- The average Jitter measured over links in the network.
- The average Delay measured over links in the network.
- The average Packet Loss measured over links in the network.

#### Quality Distribution pie chart

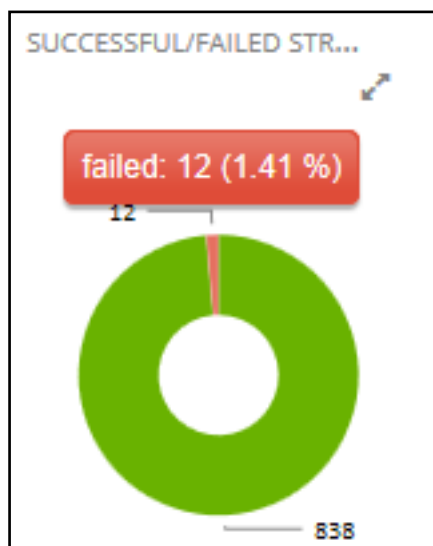
- Point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of streams over links in the network whose quality was measured to be good, fair or poor respectively. For example:



- Click any color-coded voice quality segment to open the Calls List filtered by that voice quality score (Good, Fair or Poor).

#### Successful/Failed Streams pie chart

- Point your cursor over a green or red segment; a pop-up indicates the # and % of streams over links in the network whose performance was measured to be successful or failed respectively. For example:



- Click any color-coded segment to open the Calls List filtered by that call performance evaluation (Successful or Failed).
- Click the **Devices** tab to display:
  - The total # of calls over devices in the network.
  - The maximum # of concurrent calls over devices in the network.

- The average MOS measured over devices in the network.
- The average Jitter measured over devices in the network.
- The average Delay measured over devices in the network.
- The average Packet Loss measured over devices in the network.

**Quality Distribution pie chart**

- Point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of calls over devices in the network whose quality was measured to be good, fair or poor respectively.

**Successful/Failed Streams pie chart**

- Point your cursor over a green or red segment; a pop-up indicates the # and % of calls over devices in the network whose performance was measured to be successful or failed respectively.

**■ Click the **Endpoints** tab to display:**

- The total # of calls over endpoints in the network.
- The maximum # of concurrent calls over endpoints in the network.
- The average MOS measured over endpoints in the network.
- The average Jitter measured over endpoints in the network.
- The average Delay measured over endpoints in the network.
- The average Packet Loss measured over endpoints in the network.

**Quality Distribution pie chart**

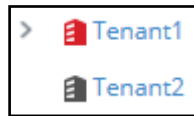
- Point your cursor over a green, yellow or red segment; a pop-up indicates the # and % of calls over endpoints in the network whose quality was measured to be good, fair or poor respectively.

**Successful/Failed Endpoints pie chart**

- Point your cursor over a green or red segment; a pop-up indicates the # and % of calls over endpoints in the network whose performance was measured to be successful or failed respectively.

## Assessing Health from the Network Topology Page

The Network Topology page lets you assess overall network health at a glance. The 'tree' in the left window of the page displays an aggregation of statuses in the network, up to the level of region. This is the first-level navigation window:



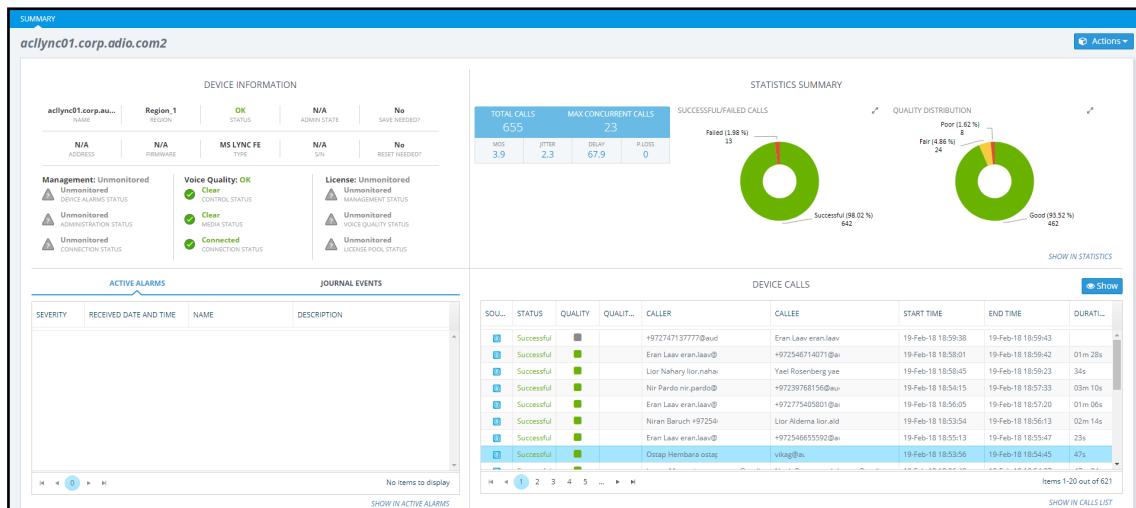
A red-coded tenant icon indicates that there is an alarm in the tenant, or that an OVOC threshold for voice quality has been exceeded in the tenant. This is the first-level navigation level.

In the middle window, a red-coded icon indicates that there is an alarm on a device, or that an OVOC threshold for voice quality has been exceeded on a device. This is the second-level navigation window:



The window lets you quickly drill down from a region to the core of an issue in a device. Very fast access to very specific information facilitates efficient network management and network optimization. For this reason, OVOC is an 'expert system'. A dynamic tab added to the menu bar provides easy future access to that specific information, facilitating troubleshooting:

**Figure 6-4: Dynamic Tab for Quick Future Access to Device Information**



Use the following table as reference to the page section 'Device Information' shown in the preceding figure.

**Table 6-1: Device Information**

Info About	Status Type	Description	Values
Management	Device Alarm Status	Indicates the severity status of the device's alarm, reported by the device; usually this is the maximum severity of the device's active alarm.	<ul style="list-style-type: none"> <li>Critical</li> <li>Major</li> <li>Minor</li> <li>Warning</li> <li>Indeterminate</li> <li>Clear</li> </ul>

Info About	Status Type	Description	Values
	Administration Status	Indicates the status of the device's administration	<ul style="list-style-type: none"> <li>■ Locked</li> <li>■ Unlocked</li> </ul>
	Connection Status	Indicates the status of the device's SNMP connectivity	<ul style="list-style-type: none"> <li>■ Connected</li> <li>■ Not Connected</li> </ul>
Voice Quality	Control Status	Indicates the status of the calls control as defined in the QoE Status and Alarm rule for this device	<ul style="list-style-type: none"> <li>■ Unmonitored</li> <li>■ Clear</li> <li>■ Major</li> <li>■ Critical</li> </ul>
	Media Status	Indicates the status of the calls media as defined in the QoE Status and Alarm rule for this device	<ul style="list-style-type: none"> <li>■ Unmonitored</li> <li>■ Clear</li> <li>■ Major</li> <li>■ Critical</li> </ul>
	Connection Status	Indicates the status of the QoE connection	<ul style="list-style-type: none"> <li>■ Not Defined – the device never connected for calls sending</li> <li>■ Connected – device is currently connected and sending calls</li> <li>■ Not Connected – device was disconnected; possible reasons: time synchronization between device and OVOC server, device was connected but for some reason closed the connection (disabled QoE reporting)</li> </ul>
License	Management Status	Indicates the status of the license management	<ul style="list-style-type: none"> <li>■ Not Defined</li> <li>■ Managed - device license contains management license</li> <li>■ Unmanaged - device license does not contain management license</li> </ul>
	Voice Quality Status	Indicates the status of the voice quality	<ul style="list-style-type: none"> <li>■ Not Requested – device does not require a Voice Quality License</li> </ul>

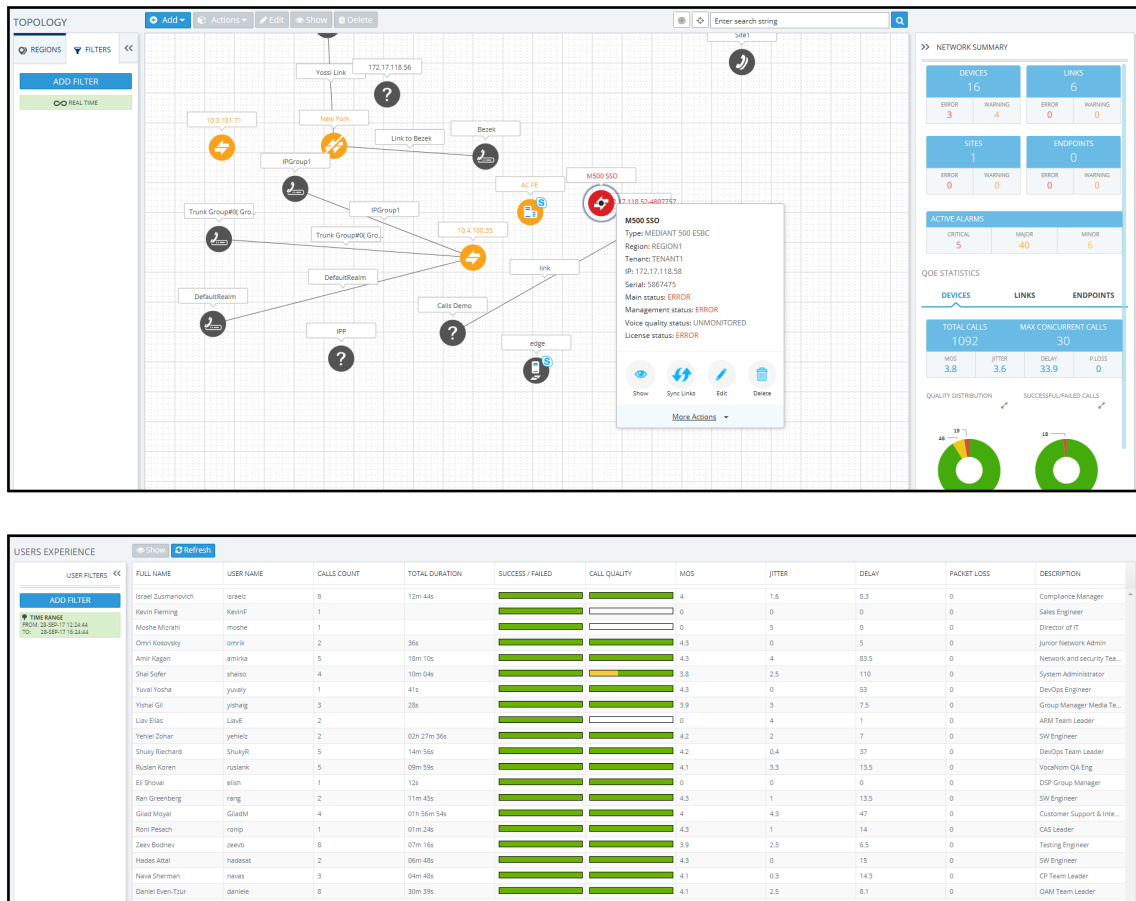
Info About	Status Type	Description	Values
			<ul style="list-style-type: none"> <li>■ Managed – device requires and receives a Voice Quality License from the OVOC server</li> <li>■ Unmanaged – device requires a Voice Quality license but the OVOC server can't assign a license for this device</li> </ul>
	OVOC License Status	Indicates the status of the OVOC license	<ul style="list-style-type: none"> <li>■ Unmanaged</li> <li>■ If License Pool is configured (same status as the status in the Fixed License Pool table)</li> <li>■ If Floating License is configured (same status as the status in the Floating License table)</li> </ul>

- For information about the page section 'Device Calls', see [Accessing the Calls List](#) on page 226. The page section 'Device Calls' mirrors the Calls List page. In the page section 'Device Calls', you can select a call made over this device and then click the **Show** button to display that call's details.
- For information about the page section 'Statistics Summary', see [Viewing Statistics on Calls over Devices](#) on page 184 and specifically [Statistics Summary](#) on page 187. The page section 'Statistics Summary' mirrors the Statistics Summary pane in the Devices Statistics page.
- For information about the page section 'Active Alarms | Journal Events', see [Monitoring Active Alarms to Determine Network Health](#) on page 155 and [Viewing Journal Alarms to Determine Operator Responsibility](#) on page 163. The page section 'Active Alarms | Journal Events' mirrors the Active Alarms page and the Journal Alarms page.

## Filtering to Access Specific Information

You can filter OVOC pages to quickly access specific information. Filters let you exclude unwanted information so that only the specific information you need is displayed. An example of a filter is *Time Range*, available in the Network Topology, Alarms, Calls List and Users Experience pages.

**Figure 6-5: Real Time | Time Range**



- **Real Time.** Pages by default display real time network information. Pages continuously refresh, presenting up-to-date network information – statistics|calls|history alarms - collected over the last 3 hours (default).
- **Add Filter > Time Range.** The page displays network information collected over a time range you specify, e.g., 10:17 - 1:17. The page is fixed. It does not keep updating and is not refreshable. See also the 'Pin all selected' feature described in the table in [Filtering by 'Time Range'](#) on the next page.

## Filtering by 'Time Range'

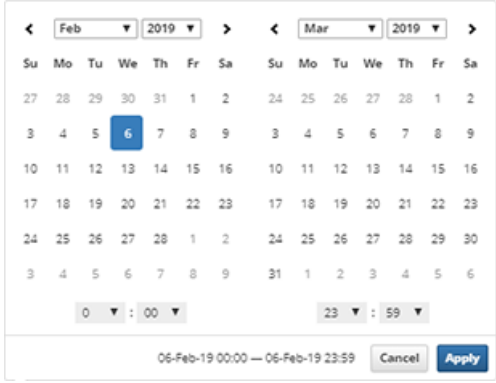
You can filter the Network Topology page and other pages by 'Time Range'. The 'Time Range' filter allows you to display *time range specific* information on the page.

**Figure 6-6: Time Range Filter**

Use the following table as reference.

**Table 6-2: Time Range Filter**

Filter Feature	Description
Pin all selected	Select this option (default) to 'preserve' the filter; the filter will remain displayed <i>in every page</i> whose tab you click. If you clear the option, the filter will only apply <i>locally</i> - to the page in which you apply the filter. The feature facilitates troubleshooting.
Back to real time	The link is enabled when you select a filter. Clicking the link removes the filter; the OVOC returns to real time.
Last 3   6   12   24 hours	Select one of these 'quick' filters in order to present only network data collected over the last 3   6   12   24 hours, to the exclusion of all other times.
Custom	You can customize dates and times by which to filter. Select <b>Custom</b> and then click the drop-down field below it.

Filter Feature	Description
	 <p>In the calendar on the left, select from when to filter: Choose a month and a day and optionally enter a time – the hour and the minutes past the hour. In the calendar on the right, select until when to filter: Choose a month and day and optionally enter the time – the hour and the minutes past the hour. Click <b>Apply</b>.</p>
Apply	Click to implement the filter. To remove the filter if necessary, click the <b>Back to real time</b> link – see above.



- There is no limitation on the time you can define.
- If you define a time range of up to (and including) six hours, the OVOC will calculate and display in the page a summation of all statistics calculated for all five-minute intervals in the range. The interval that is in process when you define the filter will not be included in the calculation. Only complete five-minute intervals will be included in the calculation.
- If you define a time range of between six and 48 hours, the OVOC will calculate and display in the page a summation of all statistics calculated for all one-hour intervals in the range. The interval that is in process when you define the filter will not be included in the calculation. Only complete one-hour intervals will be included in the calculation.
- If you define a time range of more than 48 hours, the OVOC will calculate and display in the page a summation of all statistics calculated for all one-day intervals in the range. The interval that is in process when you define the filter will not be included in the calculation. Only complete one-day intervals will be included in the calculation.

## Filtering by 'Topology'

Filtering can be performed according to 'Topology'.

**Figure 6-7: Topology**

TIME RANGE >

TOPOLOGY v

☒ Pin all selected

Search by Name, IP or Serial Number

- ErezTenantz
- test\_tenant\_492860
- test\_tenant\_532343
- no\_enough\_license
- test\_tenant\_407198a
- Ron
- test\_tenant\_733204a
- test\_tenant\_592418a
- test\_tenant\_385362a
- test\_tenant\_672237a
- test\_tenant\_2378a
- test\_tenant\_147977a** ▼
- test\_tenant\_439237a

STATUS >

MORE FILTERS >

APPLY

**Table 6-3: Topology Filter**

Filter Feature	Description
Pin all selected	Select this option (default) in order to 'preserve' the filter; the filter will remain displayed in every screen whose tab you click. If you clear the option, the filter will only apply to the screen in which you apply the filter. The feature facilitates troubleshooting. After the filter is applied, the OVOC becomes non real time.
Search	<ul style="list-style-type: none"> <li>■ Enter a search string; all information is filtered out except for the information related specifically to the string you entered.</li> <li>■ In every page in which there is a Topology filter, you can search according to IP address or serial number. <ul style="list-style-type: none"> <li>● Enter the IP address of the entity to search for; the entity whose IP address you entered is displayed. Use the figure here as reference. Click the arrow adjacent to the entity to view in a pop-up window information about the entity and to decide if this entity is the one you are looking for. In the pop-up window, you can also choose to perform management actions from the row of action icons displayed lowermost.</li> </ul> </li> </ul>

Filter Feature	Description
	<div data-bbox="443 282 1409 730"> </div> <p>■ Enter the Serial Number of the entity to search for; the entity whose SN you entered is displayed. Click the arrow adjacent to the entity to view information about the entity in a pop-up window and to decide if this entity is the one you are looking for. In the pop-up window, you can also choose to perform management actions from the row of action icons displayed lowermost.</p> <p>Note that the option to search per IP address and Serial Number is available in all pages / windows in which there is a Topology tree. In the Alarms Forwarding Rules Details screen, for example, the <b>Open Topology Tree</b> button opens a window whose search field can be searched per IP address and SN.</p> <div data-bbox="488 1061 1434 1765"> </div>
'Tenant'	<p>Filters the page according to the tenant. At least one tenant is always defined – see <a href="#">Network Architecture</a> on page 2 for an explanation of multi-tenancy architecture.</p> <p>Allows you to filter further, according to entities defined under the tenant.</p>

## Filtering by 'Status'

The 'Status' filter enables you to filter a page. The filter applies to the pages under the **Network** menu: Topology, Devices – Manage, Links and Endpoints – Status pages.

**Figure 6-8: Alarm 'Status' Filter**

TIME RANGE >

TOPOLOGY >

STATUS ▾









- ☒ OK
- ☒ WARNING
- ☒ ERROR
- ☒ UNMONITORED

MORE FILTERS >

APPLY

Use the following table as reference.

**Table 6-4: Status Filter**

Filter	Description
OK	Select to display entities whose status is clear (OK), color coded green, for example,  indicates a tenant whose status is 'OK' and  indicates a region whose status is 'OK'.
WARNING	Select to display entities whose status is warning, color coded orange, for example,  indicates a tenant whose status is 'Warning' and  indicates a region whose status is 'Warning'.
ERROR	Select to display entities whose status is error, color coded red, for example,  indicates a tenant whose status is Error and  indicates a region whose status is Error.
UNMONITORED	Select to display entities whose status is unmonitored, color coded black, for example,  indicates a tenant whose status is 'Unmonitored' and  indicates a region whose status is 'Unmonitored'.

## Filtering by 'More Filters'

You can filter a page by 'More Filters'.

**Figure 6-9: More Filters – Network Topology Page**

Use the following table as reference.

**Table 6-5: More Filters - Network Topology Page**

Filter	Description
Managed by license pool	From the drop-down list, select either <b>Both</b> , <b>Managed</b> or <b>Not managed</b> .
Device family type	From the drop-down list, select the device's family type to display on the page: AudioCodes Devices, SmartTAP Devices, UMP Devices, CloudBond Devices, Skype Devices, Generic Devices, or Unknown Devices. Alternatively, enter a search string.
Device type	From the drop-down list, select the device type to display on the page, for example, Mediant 2000.
Link type	From the drop-down list, select <b>IPGroup</b> , <b>Trunk Group</b> , <b>Phone Prefix</b> , <b>Control IP</b> , <b>Media IP</b> , <b>Media Realm</b> or <b>Remote Media Subnet</b> to display on the page.

## Determining Network Health from Alarms

The Active Alarms page facilitates management of all alarms currently active in the IP telephony network. Management includes performing actions such as deleting, acknowledging and saving alarms to file, as well as monitoring active alarms in the network to determine network health.

## Configuring Alarm Settings

For information on how to configure the way alarms and events are displayed in the Alarms pages, see [Configuring Alarms Settings](#) on page 69.

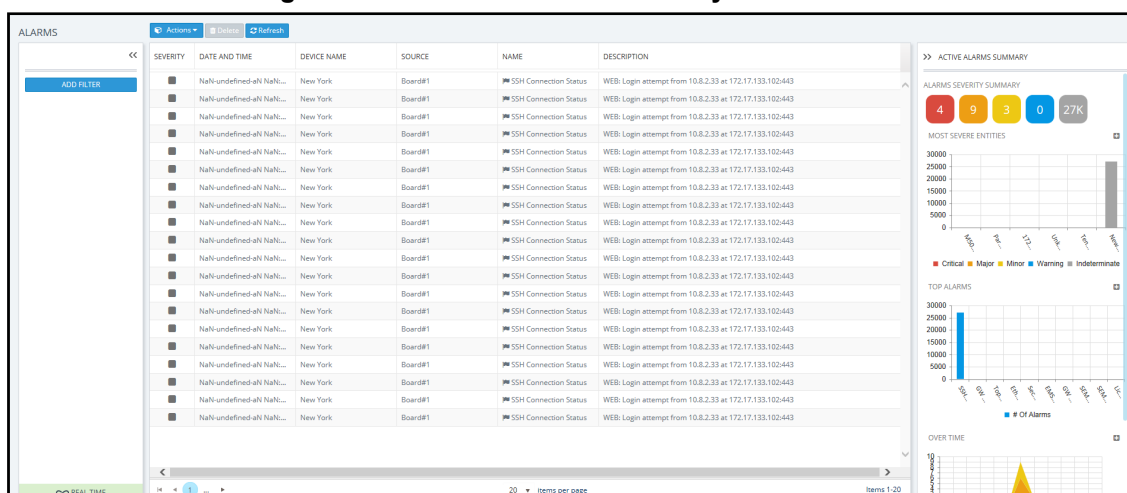
## Monitoring Active Alarms to Determine Network Health

The Active Alarms page's Active Alarm Summary pane lets you effectively monitor all the active alarms of all severities in the IP telephony network.

- **To monitor the active alarms:**

1. Open the Active Alarms page (**Alarms > Active**) and locate the Active Alarms Summary pane on the right side of the page.

### Figure 6-10: Active Alarms Summary



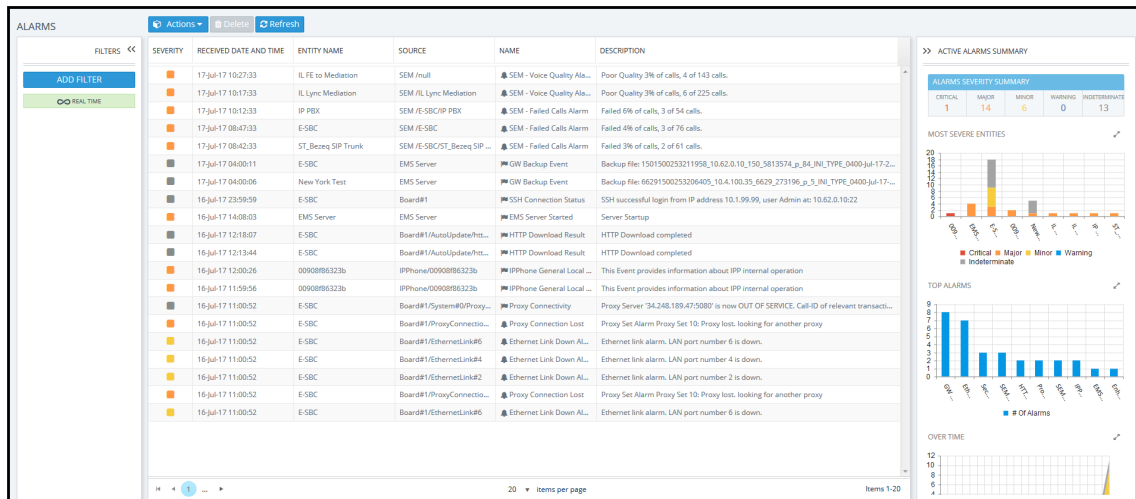
## Performing Management Actions on Active Alarms

The Active Alarms page lets you perform management actions on all alarms currently active in the network, including deleting, acknowledging, and saving alarms to file.

- To perform management actions on active alarms:

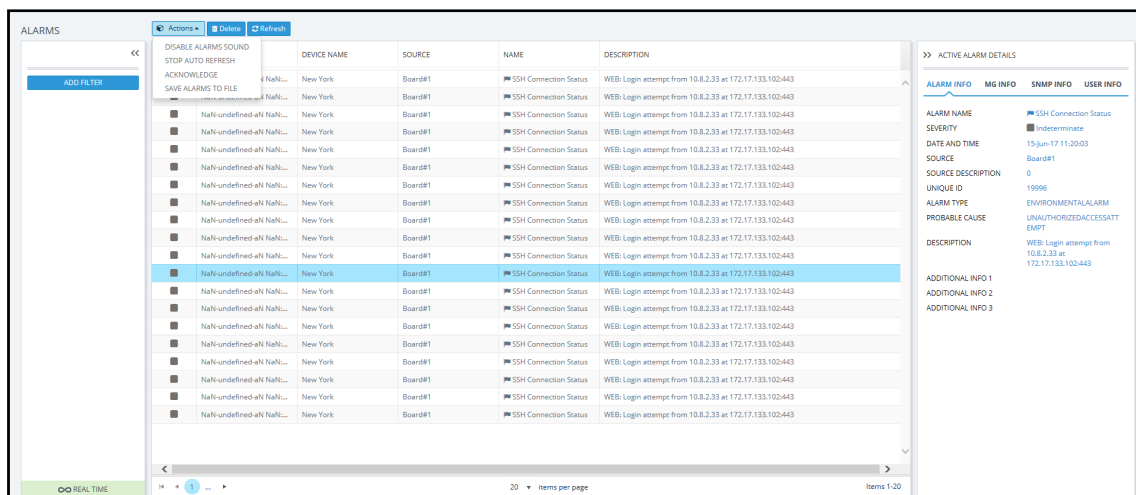
1. Open the Active Alarms page (**Alarms > Active**).

Figure 6-11: Alarms - Active



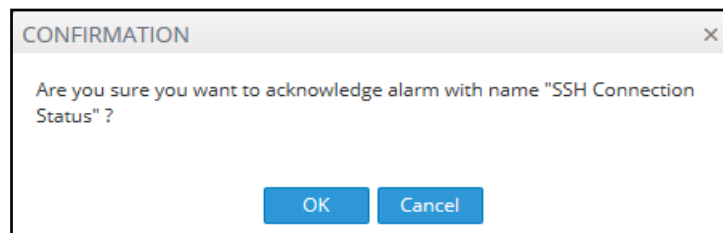
- Optionally filter the page by Topology (see [Filtering by 'Topology'](#) on page 150), Severity (see [Filtering by 'Status'](#) on page 152), Source Type (see [Filtering by 'Severity'](#) on page 158), or More Filters (see [Filtering by 'More Filters'](#) on page 161), and then select an alarm or multiple alarms and click **Actions**.

Figure 6-12: Alarms - Actions



- Select **Acknowledge** to acknowledge an alarm.

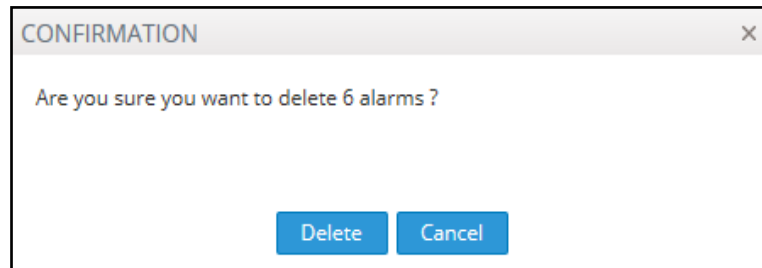
Figure 6-13: Acknowledge Alarm Confirmation



- Select **Save Alarms to File** to save alarms to file for future reference.

➤ **To delete an alarm or multiple alarms:**

- In the Active Alarms page, select the alarm or multiple alarms to delete, and click the **Delete** button.

**Figure 6-14: Delete Alarms Confirmation**

- **To refresh the page:**
  - In the Active Alarms page, select **Refresh**.
- **To enable audial alert on incoming alarms:**
  - From the **Actions** drop-down, select **Enable Alarms Sound**.
- **To disable audial alerts:**
  - From the **Actions** drop-down, select **Disable Alarms Sound**.
- **To stop automatic refresh:**
  - From the **Actions** drop-down, select **Stop Automatic Refresh**.

## Filtering by 'Severity'

The 'Severity' filter applies to the pages under the **Alarms** menu: Active, Journal and History pages.

**Figure 6-15: Alarm 'Severity' Filter**

TIME RANGE >

TOPOLOGY >

SOURCE TYPE >

SEVERITY ▾

Invert | All | None

☒ Critical

☒ Major

☒ Minor

☒ Warning

☒ Indeterminate

☒ Clear

MORE FILTERS >

APPLY

The 'Severity' filter lets you select

- one severity level
- more than one severity levels
- all severity levels (**All**)
- no severity levels (**None**)

The 'Severity' filter also lets you *invert* a selection (**Invert**). If you select **Invert** after filtering (for example) for

- **All**, then all severity levels previously selected will be cleared.
- **None**, then all severity levels previously cleared will be selected.
- **Critical**, then the 'Critical' severity level previously selected will be cleared and all other levels will be selected.

Use the following table as reference.

**Table 6-6: Severity Filter**

Filter	Description
Critical	Select to display entities whose alarm severity level is critical, color coded red.
Major	Select to display entities whose alarm severity level is major, color coded orange.
Minor	Select to display entities whose alarm severity level is minor, color coded yellow.
Warning	Select to display entities whose alarm severity level is warning, color coded blue.
Indeterminate	Select to display entities whose alarm severity level is indeterminate, color coded black.
Clear	Select to display entities whose alarm severity level is clear, color coded green.

## Filtering by 'Source Type'

You can filter a page using the 'Source Type' filter. The filter applies to the Calls List page under the Calls menu and the Alarms pages. The filter lets you display calls according to the *entity from which* the calls reported to the OVOC.

**Figure 6-16: 'Source Type' Filter**

The image shows a mobile application interface for filtering calls. It features a vertical list of filter categories: 'TIME RANGE', 'TOPOLOGY', 'SOURCE TYPE', 'SEVERITY', and 'MORE FILTERS'. Each category has a right-pointing arrow. The 'SOURCE TYPE' category is currently selected and expanded, showing a list of four options, each with a checked checkbox: 'Show Devices', 'Show Sites', 'Show Links', and 'Show Endpoints'. At the bottom of the filter panel is a grey button labeled 'APPLY'.

Use the following table as reference.

**Table 6-7: 'Source Type' Filter**

Filter	Description
Show Devices	Displays only calls whose report was sent to the OVOC <i>from devices</i> .
Show Sites	Displays only calls whose SIP Publish report was sent by endpoints to the OVOC <i>from sites</i> .
Show Links	Displays only calls transmitted <i>through links</i> .
Show Endpoints	Displays only calls whose SIP Publish report was sent to the OVOC <i>from endpoints</i> .

## Filtering by 'More Filters'

**Figure 6-17: More Filters – Alarms Active Page**

TOPOLOGY >

SEVERITY >

SOURCE TYPE >

MORE FILTERS ▼

**Sources:**

**Alarms Type:**

☐ Events

Use the following table as reference.

**Table 6-8: More Filters – Alarms Active Page**

Filter	Description
Sources	Enter the name of the entity from which the alarm originated.
Alarm Type	Select the 'Events' option for the page to display only alarms that are of type events.

## Filtering by 'Type'

The 'Type' filter augments existing filtering capability in the Alarms – Active page; you can filter the page for 'Only Alarms' or 'Only Events'.

### ➤ To filter for 'Type':

1. In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Type' drop-down, select **All**, **Only Alarms** or **Only Events**.

Figure 6-18: Type Filter

2. View in the Active Alarms page, in the 'Name' column:

- Bell icons, if you filtered for 'Only Alarms'
- Flag icons, if you filtered for 'Only Events'

Figure 6-19: Type - Only Alarms - Bells in 'Name' Column

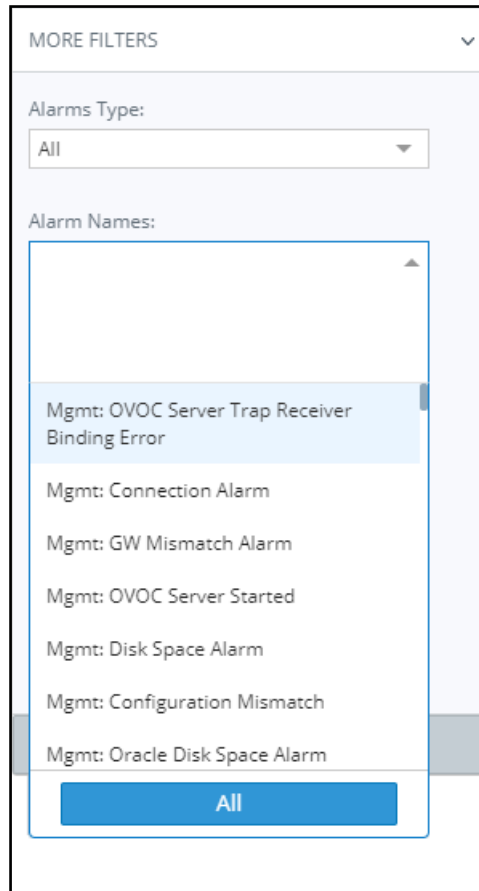
ALARMS					
<div> <div> Actions Save Delete Refresh </div> </div>					
FILTERS	SEVERITY	RECEIVED DATE AND TIME	ENTITY NAME	SOURCE	NAME
<div>ADD FILTER</div> <div>REAL TIME</div> <div>MORE FILTERS</div> <div>TYPE: ONLY ALARMS</div>		21-Feb-19 17:16:54	IL S4B FE	OVOC QoE/Device	🔔 QoE: Failed Calls Alarm
		21-Feb-19 16:28:35	00908f4818c1	IPPhone/00908f4818c1	🔔 IPPhone Lync Login Failure
		21-Feb-19 15:47:58	00908f55fd3a	IPPhone/00908f55fd3a	🔔 IPPhone Lync Login Failure
		21-Feb-19 15:46:51	NJ SBC	OVOC QoE/Device	🔔 QoE: Failed Calls Alarm
		21-Feb-19 15:46:50	NJ sfb	OVOC QoE/Link	🔔 QoE: Failed Calls Alarm
		21-Feb-19 15:46:50	Verizon	OVOC QoE/Link	🔔 QoE: Failed Calls Alarm
		21-Feb-19 15:46:50	NJ S4B FE/Mediation	OVOC QoE/Device	🔔 QoE: Failed Calls Alarm
		21-Feb-19 09:56:54	HQ SBC	OVOC QoE/Device	🔔 QoE: Failed Calls Alarm

## Filtering by 'Alarm Names'

The 'Alarm Names' filter augments already existing filtering capability in the Active Alarms page; you can filter the page by alarm name.

### ➤ To filter by 'Alarm Names':

- In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Alarm Names' drop-down, select the filter.



- In the Alarms Forwarding Rule screen (**Alarms > Forwarding > Add**), click the tab **Rule Conditions** and then from the 'Alarm Names' drop-down, select the alarm.

## Viewing Journal Alarms to Determine Operator Responsibility

The Journal Alarms page lets you view actions of operators performed historically in the OVOC up to the present. The page can help you determine if operator activity may have been responsible for an active alarm. You can then reference the History page to verify correlation (see [Viewing History Alarms](#) on page 165).

**Figure 6-20: Journal Alarms**

JOURNAL								ACTION DETAILS		
DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION	TENANT	OPERATOR		GENERAL INFO	ENTITY INFO	USER INFO
21-Feb-19 18:11:37	OVOC Mgmt	OVOC Mgmt	Security: Login	User: NATeamSystemOperator has...	System	NATeamSystemOperator		SEVERITY		
21-Feb-19 18:11:37	OVOC Mgmt	OVOC Mgmt	Security: Login	User: NATeamSystemOperator has...	System	NATeamSystemOperator		DATE AND TIME	21-Feb-19 17:01:04	
21-Feb-19 17:37:17	OVOC Mgmt	OVOC Mgmt	Security: Login	daivide logged in via OVOC from 10...	System	daivide		SOURCE	OVOC Mgmt	
21-Feb-19 17:37:09	OVOC Mgmt	OVOC Mgmt	Security: Login	User: daivide has failed to Authent...	System	daivide		NAME	Configuration: Update	
21-Feb-19 17:01:04	0090875C75D	OVOC Mgmt	Configuration: Update	Endpoint: 0090875C75D_10.15.2.5...	Adio	InternalSystem		UNIQUE ID	1290995	
21-Feb-19 17:01:03	OVOC Mgmt	OVOC Mgmt	Configuration: Add	Added 1 new Managed Endpoint: 0...	System	System		DESCRIPTION	Endpoint: 0090875C75D_10.15.2.5, updated fields: TENANT NAME = A	
21-Feb-19 16:30:22	OVOC Mgmt	OVOC Mgmt	Configuration: Add	Added 1 new Managed Endpoint: 0...	System	System				
21-Feb-19 16:18:48	OVOC Mgmt	OVOC Mgmt	Security: Login	admindemo2 logged in via OVOC f...	System	admindemo2				
21-Feb-19 16:18:39	OVOC Mgmt	OVOC Mgmt	Security: Login	acldmin logged in via OVOC from ...	System	acldmin				
21-Feb-19 16:15:41	009089A9F44	OVOC Mgmt	Configuration: Update	Endpoint: 009089A9F44_10.22.12...	Adio	InternalSystem				
21-Feb-19 16:15:40	OVOC Mgmt	OVOC Mgmt	Configuration: Add	Added 1 new Managed Endpoint: 0...	System	System				



The Journal Alarms page reflects *all actions* performed by network administrators in AudioCodes' *Device Manager*. Records of network administrator actions are sent from the Device Manager to the OVOC server to be displayed in the OVOC Journal Alarms page. See also AudioCodes' *Device Manager Administrator's Manual*.

## Filtering the Alarms Journal by 'More Filters'

You can filter the Alarms Journal page by 'More Filters'.

**Figure 6-21: More Filters – Alarms Journal Page**

The screenshot shows a mobile interface for filtering alarms. It has a list of filter categories: TIME RANGE, TOPOLOGY, SOURCE TYPE, and MORE FILTERS. The 'MORE FILTERS' category is expanded, showing two input fields: 'Sources:' and 'Operator:'. At the bottom of the expanded section is an 'APPLY' button.

Use the following table as reference.

**Table 6-9: More Filters – Alarms Journal Page**

Filter	Description
Sources	Enter the name of the entity from which the alarm originated.
Operator	Enter the name of the operator according to whom to filter.

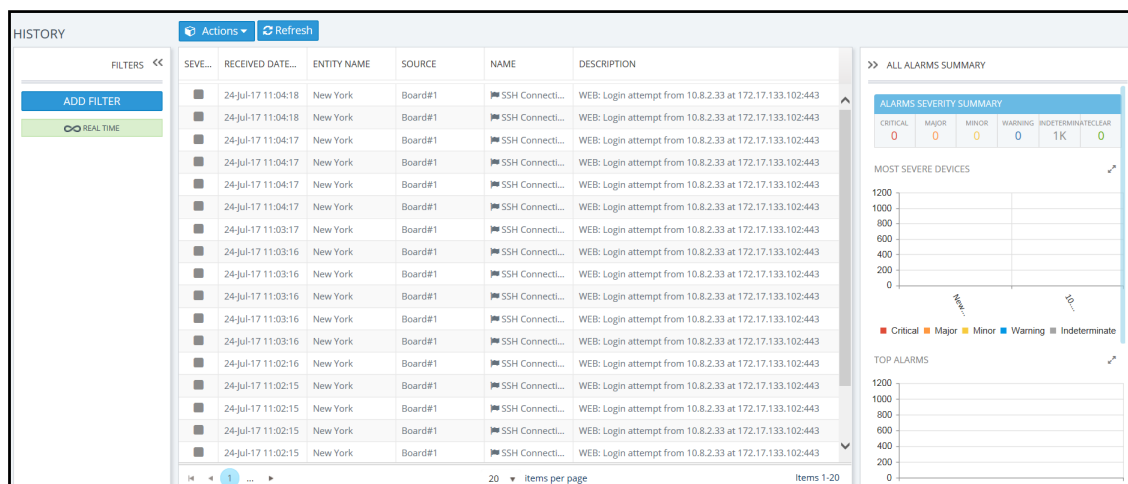
## Viewing History Alarms

The History page displays historical alarms. The page can help you verify that an operator's action was responsible for an active alarm.

➤ **To determine if an operator's action was responsible for an active alarm:**

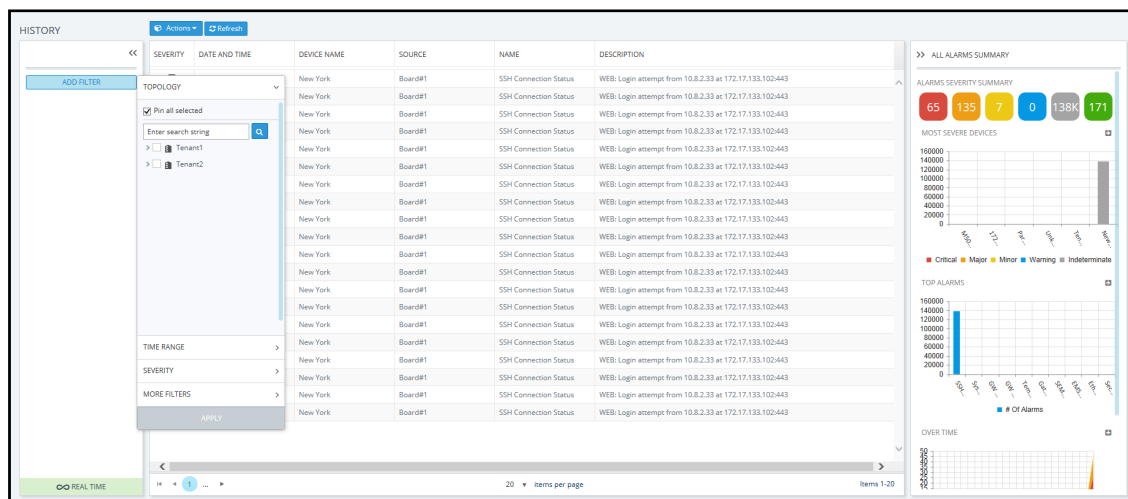
1. Open the History page (**Alarms > History**).

**Figure 6-22: Alarms - History**



2. Click **Add Filter** to filter the page according to Topology, Time Range, Severity or More Filters. For a full description of these filters, see [Filtering to Access Specific Information](#) on page 147.

**Figure 6-23: Alarms Page Filters**



## Filtering by 'Type'

The 'Type' filter augments existing filtering capability in the History Alarms page; you can filter the page for 'Only Alarms' or 'Only Events'.

### ➤ To filter for 'Type':

1. In the Active Alarms page, click **Add Filter**, choose **More Filters** and then from the 'Type' drop-down, select **All**, **Only Alarms** or **Only Events**.

Figure 6-24: Type Filter

2. In the 'Name' column in the Alarms History page, you can view:

- Bell icons, if you filtered for 'Only Alarms'
- Flag icons, if you filtered for 'Only Events'

Figure 6-25: History Alarms - Type Filter

HISTORY		Actions		Refresh		
SEVERITY	RECEIVED DATE AND TIME	ENTITY NAME	SOURCE	NAME	DESCRIPTION	
🚨	03-May-18 14:53:04	10.3.181.83-9331606	Board#1/CertificateExpiry#0	🔔 Certificate Expiry Alarm	Certificate expiry: The certificate of TLS context 0 has expired 17654 days ago.	
🟢	03-May-18 14:53:04	10.3.181.83-9331606	Board#1/CertificateExpiry#0	🔔 Certificate Expiry Alarm	Alarm cleared: Certificate expiry: The certificate of TLS context 0 has expired 17653 days ago.	
🟢	03-May-18 13:36:25	CLM_10.36.50.244	OVOC Mgmt	🔔 GW Connection Alarm	Connection established	
🟢	03-May-18 13:36:25	CLM_10.36.49.178	OVOC Mgmt	🔔 GW Connection Alarm	Connection established	
🟢	03-May-18 13:36:25	10.36.12.154	OVOC Mgmt	🔔 GW Connection Alarm	Connection established	
🟢	03-May-18 13:36:25	mimic_10.36.12.192	OVOC Mgmt	🔔 GW Connection Alarm	Connection established	
🚨	03-May-18 13:35:34	CLM_10.36.50.244	OVOC Mgmt	🔔 GW Connection Alarm	Connection Lost	
🚨	03-May-18 13:35:34	CLM_10.36.49.178	OVOC Mgmt	🔔 GW Connection Alarm	Connection Lost	
🚨	03-May-18 13:35:34	10.36.12.154	OVOC Mgmt	🔔 GW Connection Alarm	Connection Lost	
🚨	03-May-18 13:35:34	mimic_10.36.12.192	OVOC Mgmt	🔔 GW Connection Alarm	Connection Lost	
🟡	03-May-18 12:51:47	mimic_10.36.1.69	OVOC QoS/mimic_10.36.1.69	🔔 QoS: Poor Voice Qualit...	Poor Quality 7% of calls, 14 of 215 calls.	
🟢	03-May-18 12:51:47	mimic_10.36.1.69	OVOC QoS/mimic_10.36.1.69	🔔 QoS: Poor Voice Qualit...	Clearing currently active alarm before raising different severity alarm on the same source.	

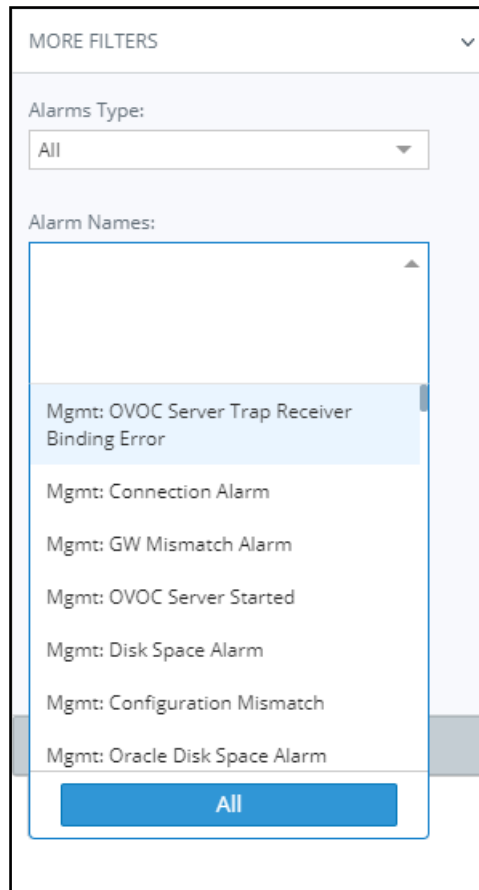
## Filtering by 'Alarm Names'

The 'Alarm Names' filter augments already existing filtering capability in the History Alarms page; you can filter the page by alarm name.

### ➤ To filter by 'Alarm Names':

1. In the Alarms History page, click **Add Filter**, choose **More Filters** and then from the 'Alarm Names' drop-down, select the filter.

**Figure 6-26: 'Alarm Names' Filter**



2. In the Alarms Forwarding Rule screen (**Alarms > Forwarding > Add**), click the tab **Rule Conditions** and then from the 'Alarm Names' drop-down, select the alarm.

## Forwarding Alarms

The Forwarding page lets you add an alarm forwarding rule. The OVOC can forward alarms to multiple destinations in these formats:

- SNMP Notifications (SNMP 1 / SNMP 2) - see [Forwarding Alarms whose Destination Type is 'SNMP'](#) on page 173
- External Mail / Internal Mail - see [Forwarding Alarms whose Destination Type is 'Mail'](#) on page 176
- Syslog - see [Forwarding Alarms whose Destination Type is 'Syslog'](#) on page 179
- Notification - see [Forwarding Alarms whose Destination Type is 'Notification'](#) on page 181

### ➤ To configure alarm forwarding:

1. Open the Alarms Forwarding page (**Alarms > Forwarding**).

**Figure 6-27: Alarms Forwarding Page**

FORWARDING <span>➕ Add</span> <span>✎ Edit</span> <span>🗑 Delete</span> <span>🔄 Refresh</span>				
RULE NAME	ACTIVE	DESTINATION TYPE	DESTINATION	TENANT
AC OVOC Server	✖	MAIL	liran.badiri@a.com,marina.Risher@a	System
politie_test	✖	SYSLOG	192.168.1.1	System
testAlarm	✔	SYSLOG	1.1.1.1	System
Gmail	✖	MAIL	liranbadiri@gmail.com	System

2. Click **Add**.

**Figure 6-28: Alarms Forwarding Rule Details – Topology Conditions**

ALARMS FORWARDING RULE DETAILS

Rule Name \*

☒ Forward matching alarms/events
☐ Prevent forwarding of matching alarms/events

Enable/Disable Rule ☒

TOPOLOGY CONDITIONS

RULE CONDITIONS

DESTINATION

Rule Owner \*
System - all tenants

Attachments:

Tenants: all Tenant/s, All / None

Regions: all Region/s, All / None

Devices: all Device/s, All / None

Links: all Link/s, All / None

Sites: all Site/s, All / None

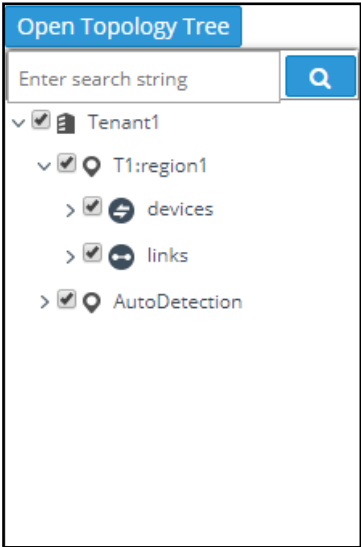
Open Topology Tree

OK

Close

3. Configure the Topology Conditions using the following table as reference:

**Table 6-10: Alarms Forwarding – Topology Conditions**

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events -or- Prevent forwarding matching alarms/events	<p>Allows or prevents forwarding alarms depending on the destination you select. If you select <b>Prevent forwarding matching alarms/events</b> and then select <b>Minor Alarms</b> from the 'Severities' drop-down under the <b>Rule Conditions</b> tab, then minor alarms are not forwarded.</p> <p>See related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarm Settings</a> on page 155</p>
Enable/Disable Rule	<p>Enables or disables the rule if the parameters and conditions configured under this tab as well as under <b>Rule Conditions</b> and <b>Destinations</b> are met.</p> <p>See related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarm Settings</a> on page 155</p>
Rule Owner	<p>From the drop-down, select <b>System – all tenants</b>; the rule will then apply to <i>all tenants</i> and to all regions/links/devices/sites under all tenants.</p> <p>Here's what you'll then view next to 'Attachments':  <b>all Tenant/s, all Region/s, all Device/s, all Link/s, all Site/s</b></p> <p>If you select a <i>specific tenant</i> from the drop-down, the rule will apply by default to <i>all entities under that specified tenant</i>.</p> <p>Click <b>Open Topology Tree</b> and then click &gt; to view the entities under that tenant and if you want, to change the default.</p>  <p>Only the operator assigned to that tenant can view and change it. The <b>All/None</b> filters next to 'Attachments' allow you to quickly specify to which entities rule forwarding will apply, if not to all.</p>

4. Click the **Rule Conditions** tab.

**Figure 6-29: Alarms – Forwarding – Rule Conditions**

ALARMS FORWARDING RULE DETAILS

Rule Name \*

☒ Forward matching alarms/events

☐ Prevent forwarding of matching alarms/events

Enable/Disable Rule

☒

TOPOLOGY CONDITIONS

RULE CONDITIONS

DESTINATION

Alarm Origin

All Selected

☐ none

Event Origin

All Selected

☐ none

Severities

All Selected

Alarm Names

All Selected

Alarm Types

All Selected

OK

Close

5. Configure the screen using the following table as reference.

**Table 6-11: Forwarding Alarms – Rule Conditions - Parameter Descriptions**

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events -or- Prevent forwarding matching alarms/events	<p>Allows or prevents forwarding alarms depending on the destination you select. If you select <b>Prevent forwarding matching alarms/events</b> and then select <b>Minor Alarms</b> from the 'Severities' drop-down under the <b>Rule Conditions</b> tab, then minor alarms are not forwarded.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarm Settings</a> on page 155</p>
Enable/Disable Rule	<p>Enables or disables the rule if the parameters and conditions configured under this tab as well as under <b>Rule Conditions</b> and <b>Destinations</b> are met.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarm Settings</a> on page 155</p>
Alarm Origin	<p>Select the origin from which alarms will be forwarded:</p> <ul style="list-style-type: none"> <li>■ Management</li> <li>■ QoE</li> <li>■ Devices</li> <li>■ Endpoints</li> </ul>
Event Origin	<p>Select the origin from which events will be forwarded:</p> <ul style="list-style-type: none"> <li>■ Management</li> <li>■ QoE</li> <li>■ Devices</li> <li>■ Endpoints</li> </ul>
Severities	<p>From the 'Severities' drop-down, select the severity level of the alarms you want to receive:</p> <ul style="list-style-type: none"> <li>■ Warning</li> <li>■ Minor</li> <li>■ Major</li> <li>■ Critical</li> <li>■ Indeterminate</li> </ul> <p>Default: All Selected.</p>
Alarm Names	<p>Allows forwarding alarms according to specific alarm names. For example, if you select <b>Power Supply Failure</b> then only this alarm will be forwarded. Default: <b>All Selected</b>. The search field lets you find an alarm according to name or origin.</p>

Parameter	Description
Alarm Types	Allows forwarding alarms according to specific alarm types. For example, if you select <b>communicationsAlarm</b> then only this alarm type will be forwarded. Default: <b>All Selected</b> . The search field lets you find an alarm according to type.
Source	Free text box that allows you to filter according to alarms' 'Source' field (identical to the 'Source' column displayed in the Alarms History page).

6. Click the **Destination** tab.

## Forwarding Alarms whose Destination Type is 'SNMP'

The SNMP forwarding option is typically used for integration of the OVOC with a Network Management System (NMS). For more information about forwarding SNMP notifications, see the *OAM Integration Guide*. After selecting the **Destination** tab, the screen whose destination type is SNMP v2 or SNMP v3 opens by default.

**Figure 6-30: Alarms – Forwarding – Destination Type - SNMP v2**

**ALARMS FORWARDING RULE DETAILS** [X]

Rule Name \*

☒ Forward matching alarms/events ☐ Prevent forwarding of matching alarms/events

Enable/Disable Rule ☒

**TOPOLOGY CONDITIONS** **RULE CONDITIONS** **DESTINATION**

Destination Type \* SNMP

Destination Details

Destination Host IP Address \*

Destination Host Port 162

☒ SNMP v2 ☐ SNMP v3

Trap Community

OK Close

**Figure 6-31: Alarms – Forwarding – Destination Type - SNMP v3**

**ALARMS FORWARDING RULE DETAILS** [X]

Rule Name \*

☒ Forward matching alarms/events
 ☐ Prevent forwarding of matching alarms/events

Enable/Disable Rule ☒

**TOPOLOGY CONDITIONS**      **RULE CONDITIONS**      **DESTINATION**

---

Destination Type \* SNMP ▼

Destination Details

Destination Host IP Address \*

Destination Host Port 162

☐ SNMP v2    ☒ SNMP v3

Security Name \*

Security Level \* No Security ▼

Authentication Protocol No Protocol ▼

Authentication Key

Privacy Protocol None ▼

Privacy Key

OK Close

Use the following table as reference for the 'Destination Type' parameter.

**Table 6-12: Forwarding Alarms – Destination**

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events -or- Prevent forwarding matching alarms/events	<p>Allows or prevents forwarding alarms depending on the destination you select. If you select <b>Prevent forwarding matching alarms/events</b> and then select <b>Minor Alarms</b> from the 'Severities' drop-down under the <b>Rule Conditions</b> tab, then minor alarms are not forwarded.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69</p>

Parameter	Description
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under <b>Rule Conditions</b> and <b>Destinations</b> are met. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69
Destination Type	Determines the format in which the alarm or event will be forwarded. From the drop-down, select <ul style="list-style-type: none"><li>■ SNMP (default)<ul style="list-style-type: none"><li>✓ SNMP v2</li><li>✓ SNMP v3</li></ul></li><li>■ MAIL</li><li>■ SYSLOG</li></ul>

## Forwarding Alarms whose Destination Type is 'Mail'

➤ **To forward alarms whose destination is 'Mail':**

1. In the Alarms Forwarding Rule Details screen, select **MAIL** from the 'Destination Type' drop-down.

**Figure 6-32: Alarms Forwarding Rule Details – Destination – Mail**

The screenshot shows a dialog box titled "ALARMS FORWARDING RULE DETAILS" with a close button (X) in the top right corner. The dialog is divided into three tabs: "TOPOLOGY CONDITIONS", "RULE CONDITIONS", and "DESTINATION". The "DESTINATION" tab is currently selected and highlighted with a blue border. Below the tabs, the "Destination Type" is set to "MAIL" in a dropdown menu. Below this, there is a section titled "Destination Details" which contains several fields: "Use Internal Mail Server" (with an unchecked checkbox), "Mail Host" (text input), "Mail Host Username" (text input), "Mail Host Password" (text input), "From" (text input), and "To" (a larger text area). At the bottom of the dialog, there are two buttons: "OK" and "Close".

2. Select the **Use Internal Mail Server** option.

**Figure 6-33: Alarms Forwarding Rule Details – Destination – Mail – Use Internal Mail Server**

ALARMS FORWARDING RULE DETAILS

Rule Name \*

☒ Forward matching alarms/events

☐ Prevent forwarding of matching alarms/events

Enable/Disable Rule

☒

TOPOLOGY CONDITIONS

RULE CONDITIONS

DESTINATION

Destination Type \*

MAIL

Destination Details

Use Internal Mail Server

☒

Mail Host

Mail Host Username

Mail Host Password

From

To \*

OK

Close

3. Configure the parameters using the following table as reference.

**Table 6-13: Forwarding Alarms - Destination – Mail**

Parameter	Description
Use Internal Mail Server	<p>If this option is selected, all the fields in this table following will be deactivated, except the 'To' field. If selected, it'll only be necessary to configure the internal mail server as the destination to which to forward alarms; it'll be unnecessary to configure a mail host. If the option is cleared, all the fields in the table following will be activated.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69</p>
Mail Host	Enter the <b>Mail Host IP address or FQDN</b> (e.g., smtp.office365.com).
Mail Host Username	Enter the <b>mail host username</b> .
Mail Host Password	Enter the <b>mail host password</b> .
From	<p>Enter the <b>e-mail address</b> the recipient will see when the mail arrives.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69</p>
To	<p>Enter the <b>list of email addresses</b> (coma separated) to which to send mail. If the option 'Use Internal Mail Server' is selected, 'To' will be the only parameter activated; all others will be deactivated. In this case, configure the internal mail server as the destination to which to forward alarms.</p> <p>See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69</p>

4. Click **OK**; alarms are forwarded to specified email destinations in the following email format:

Title: New <Alarm/Event> <Alarm Name>, received from <Node Name> with Severity <Severity>  
 Message body: will include all the fields we have today in Alarm Item

## Forwarding Alarms whose Destination Type is 'Syslog'

Alarms can be forwarded to the Syslog destination type.

➤ **To forward alarms whose Destination Type is 'Syslog':**

1. In the Alarms Forwarding Rule Details screen, select **SYSLOG** from the 'Destination Type' drop-down.

**Figure 6-34: Destination Type 'Syslog'**

The screenshot shows a window titled "ALARMS FORWARDING RULE DETAILS" with a close button (X) in the top right corner. The window is divided into three tabs: "TOPOLOGY CONDITIONS", "RULE CONDITIONS", and "DESTINATION". The "DESTINATION" tab is currently selected and highlighted in blue. Below the tabs, there are several input fields and checkboxes. At the top, there is a "Rule Name \*" field. Below it, there are two radio buttons: "Forward matching alarms/events" (selected) and "Prevent forwarding of matching alarms/events". Below the radio buttons, there is a checkbox labeled "Enable/Disable Rule" which is checked. The "DESTINATION" tab contains a "Destination Type \*" dropdown menu with "SYSLOG" selected. Below this, there is a section titled "Destination Details" which contains two input fields: "Syslog Host IP Address \*" and "Syslog Host Port". The "Syslog Host Port" field has the value "1" entered. At the bottom of the window, there are two buttons: "OK" and "Close".

2. Configure the parameters using the following table as reference.

**Table 6-14: Forwarding Alarms - Destination – Syslog**

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events -or- Prevent forwarding matching alarms/events	Allows or prevents forwarding alarms depending on the destination you select. If you select <b>Prevent forwarding matching alarms/events</b> and then select <b>Minor Alarms</b> from the 'Severities' drop-down under the <b>Rule Conditions</b> tab, then minor alarms are not forwarded.  See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under <b>Rule Conditions</b> and <b>Destinations</b> are met.  See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69
Syslog Host IP Address	Enter the IP address of the Syslog host.
Syslog Host Port	Enter the port of the Syslog host.

3. Click **OK**; alarms are forwarded to Syslog.

Syslog features a well-defined message format structure detailed in RFC 3164. The OVOC'S severity levels are adjusted to the severity levels of the Syslog protocol. The following table maps the two:

Critical	Alert
Major	Critical
Minor	Error
Warning	Warning
Indeterminate	Informational
Clear	Notice

The message part of the Syslog protocol contain this structure:

Title: <Alarm/Event> <Alarm Name>, received from <Node Name, Node IP> with Severity <Severity>.  
Description: <Source>, <Description>

If the alarm is forwarded from the source global IP address in an HA configuration, the device IP is the global IP address.

## Forwarding Alarms whose Destination Type is 'Notification'

Alarms can be forwarded to the 'Notification' destination type. After configuring this destination type, notifications will automatically pop up in the OVOC GUI when alarms are received.

➤ **To forward alarms whose Destination Type is 'Notification':**

1. In the Alarms Forwarding Rule Details screen under the **DESTINATION** tab, select **NOTIFICATION** from the 'Destination Type' drop-down.

**Figure 6-35: Destination Type 'Notification'**

The screenshot shows the 'ALARMS FORWARDING RULE DETAILS' dialog box with the 'DESTINATION' tab selected. The 'Rule Name' is 'Adding Topology'. The 'Forward matching alarms/events' radio button is selected. The 'Enable/Disable Rule' checkbox is checked. The 'Destination Type' is set to 'NOTIFICATION'. The 'Assigned Operators' list contains 'marina'. The 'Destination Details' section is empty. The 'OK' and 'Close' buttons are at the bottom.

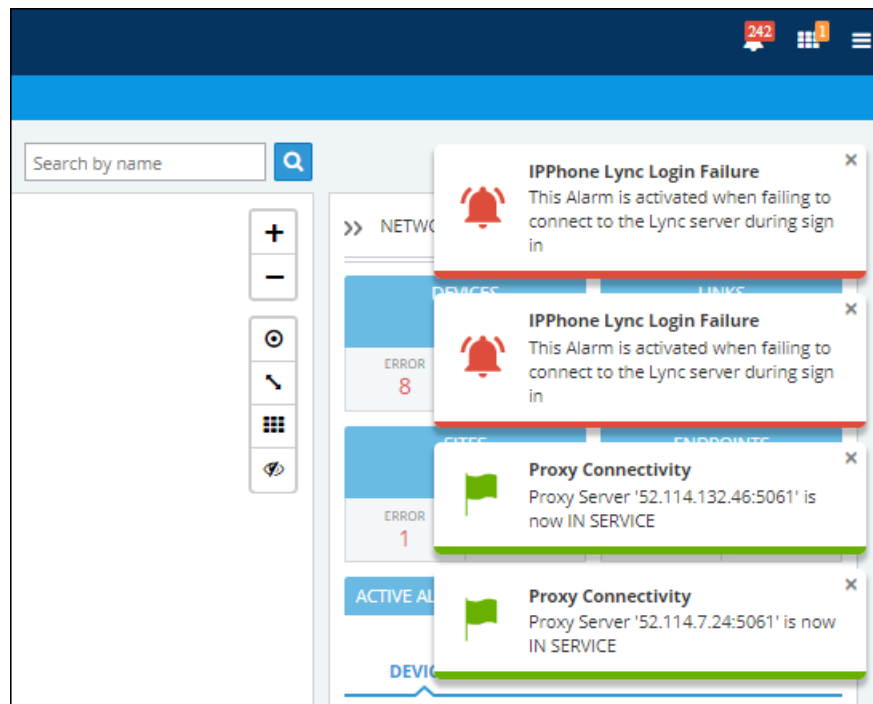
TOPOLOGY CONDITIONS	RULE CONDITIONS	DESTINATION
		<p>Destination Type *</p> <p>NOTIFICATION</p> <p>Destination Details</p> <p>Assigned Operators</p> <p>marina</p>

2. Configure the parameters using the table as reference.

**Table 6-15: Forwarding Alarms - Destination – Destination**

Parameter	Description
Rule Name	Define an intuitive name, to be displayed in the alarm summary screen.
Forward matching alarms/events -or- Prevent forwarding matching alarms/events	Allows or prevents forwarding alarms depending on the destination you select. If you select <b>Prevent forwarding matching alarms/events</b> and then select <b>Minor Alarms</b> from the 'Severities' drop-down under the <b>Rule Conditions</b> tab, then minor alarms are not forwarded. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69
Enable/Disable Rule	Enables or disables the rule if the parameters and conditions configured under this tab as well as under <b>Rule Conditions</b> and <b>Destinations</b> are met. See also related parameters 'Internal Mail Server From Address' and 'Internal Mail Server Real Name' in <a href="#">Configuring Alarms Settings</a> on page 69
Assigned Operators	Under 'Destination Details', configure the operator (or operators) to whom you want the alarm notifications to be forwarded. <b>Note:</b> <ul style="list-style-type: none"> <li>Operators whose security level is 'Admin' can assign notifications to any operator / all operators.</li> <li>Operators whose security level is 'Operator' can assign notifications only to themselves.</li> </ul>

- Click **OK**; notifications will automatically pop up in the uppermost right corner in the GUIs of all assigned operators, when alarms are received.

**Figure 6-36: Notifications Pop-up**



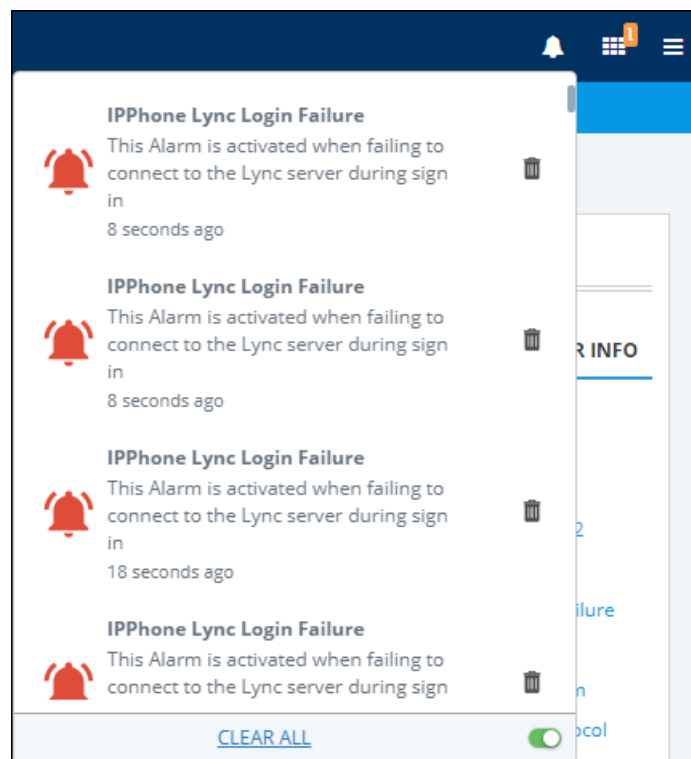
To configure the *timeout* of notification pop-ups, see [Configuring Operator Authentication Locally, in the OVOC](#) on page 34 and refer to the parameter 'Notifications display time (sec)'. The default is 3 seconds. Configuring the parameter to 0 disables the feature.

➤ **To view the notifications history:**

1. Click the bell icon in the uppermost right corner of the OVOC GUI; the icon indicates the number of notifications that have not yet been viewed; its color indicates highest alarm severity level.



2. View the alarm notifications history.



3. In the list, you can delete a notification, clear all notifications or click a notification to open the Alarms History page displaying that alarm.
4. Scroll down to view earlier notifications. Most recent notifications are listed first. Every notification indicates how long ago it was listed, e.g., **4 minutes ago**.

## Viewing the New Rules in the Alarms Forwarding Page

- The new rules are displayed in the Alarms Forwarding page (**Alarms > Forwarding**):

**Figure 6-37: New Rules in the Alarms Forwarding Page**

ACTIVE JOURNAL HISTORY FORWARDING				
FORWARDING				
<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Refresh</a>				
RULE NAME	ACTIVE	DESTINATION TYPE	DESTINATION	TENANT
testRoman	✓	SNMP	1.1.1.1	System
testRoman1	✓	SNMP	1.1.1.1	System
testRoman112	✓	SNMP	1.1.1.1	System
TEST_RULE_1	✓	SNMP	1.2.3.4	System
TEST_RULE_2	✓	SNMP	2.3.4.5	System
test111	✓	SNMP	10.4.100.100	Tenant1

## Assessing Network Health in the Statistics Pages

The OVOC graphically and textually displays network-wide statistics on call performance (% and # of calls evaluated as successful or failed), voice quality (% and # of calls whose voice quality scored good, fair or poor), etc. Statistics on calls over devices, links, sites and endpoints are displayed. The pages help operators assess and optimize network health.

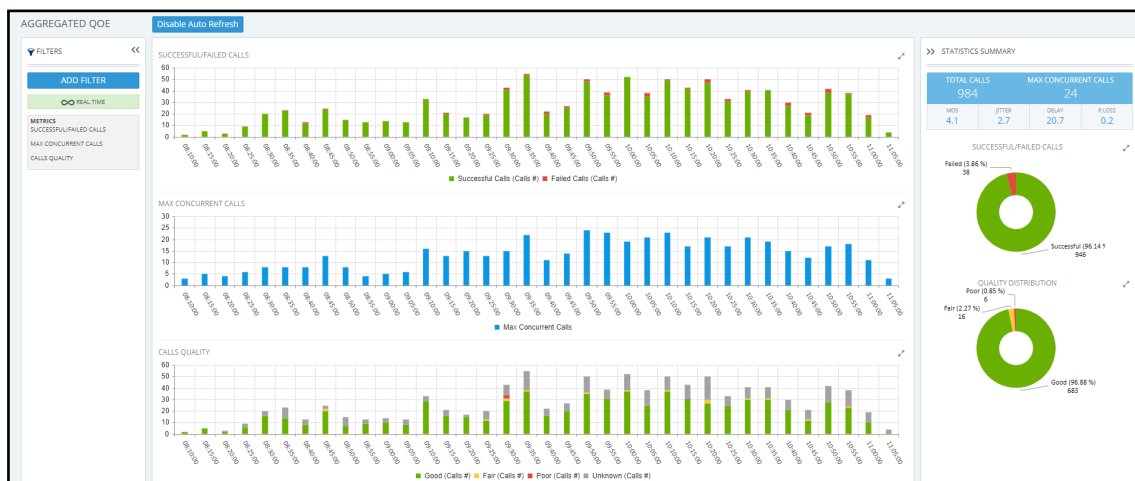
### Viewing Statistics on Calls over Devices

The Devices tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of calls over devices.

- **To view statistics on calls over devices:**

- Open the Devices Statistics page (**Statistics > Devices**).

**Figure 6-38: Devices Statistics**



You can optionally filter the page by Time Range (see [Filtering to Access Specific Information](#) on page 147) and Topology (see [Filtering by 'Topology'](#) on page 150).

The page displays (from L-R):

- Metrics (see [Metrics Bar Charts](#) on the next page)
- Bar Charts (see [Metrics Bar Charts](#) on the next page)
- Statistics Summary (see [Statistics Summary](#) on page 187)

## Metrics Bar Charts

Three metrics / bar charts are displayed by default:

- Successful / Failed Calls chart shows the % and # of calls whose performance was evaluated as successful or failed, distributed over time (see [Filtering to Access Specific Information](#) on page 147 for information about the time range filter). The chart lets you assess calls performance at a glance. The chart shows *when successful calls peaked* compared to *when failed calls peaked*. You can compare this to other charts to identify correlations.
- Max Concurrent Calls chart shows the maximum concurrent calls distributed over time. The chart shows *when* the maximum concurrent calls *peaked* compared to when they *dipped*. You can compare this to other charts to identify correlation. Max Concurrent Calls is the maximum number of calls opened at the same time in the server. Note that if you click a bar to open the Calls List page, the number of calls shown in the Calls List page might be different to the number shown in the graph; only calls that *end within the time range* are displayed in the Calls List page; if a call exceeds the time range, it won't be displayed in the Calls List page.
- Calls Quality chart shows the distribution of voice quality (% and # of calls whose voice quality scored ■ Good ■ Fair or ■ Poor) over time. Gray indicates 'Unknown' voice quality. Point the cursor over a color-coded bar segment in any time period to view this pop-up. The date and time indicates when the period ended.

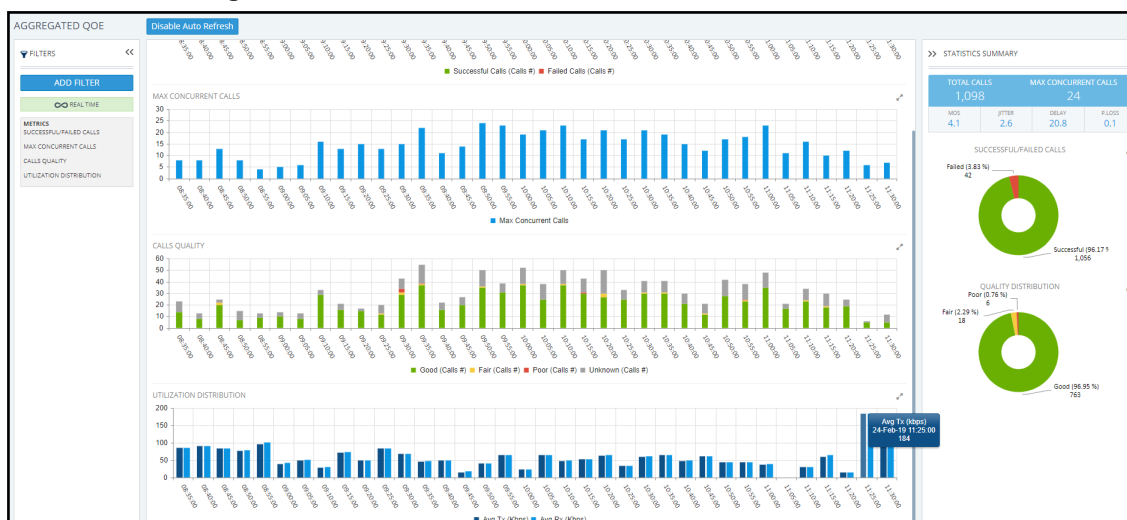
Figure 6-39: Calls Quality Bar Chart



Compare charts. If, for example, you identify a correlation over time between 'Poor' voice quality and Jitter, then Jitter is the reason for the poor voice quality.

Other metrics / bar charts that you can select and display:

- Utilization Distribution chart shows distribution of the media packets network utilization over time. A glance shows when a high rate (in Kbps) was received or transmitted (Rx/Tx rate in Kbps). The chart shows when a network is congested or uncongested, i.e., when voice quality scores may be lower. To view information on a time period, position the cursor over the bar representing the time period; the pop-up shows the date and time on which the period ended and the Rx / Tx rate in Kbps and the kilobits consumed per second during the time period:

**Figure 6-40: Utilization Distribution Bar Chart**

- Average Call Duration (ACD) chart shows distribution of ACD in the network over time. Point your mouse over a bar to determine average call duration in that time interval.
- MOS chart. Point your mouse over a bar to determine the average MOS scored in that time interval.
- Packet Loss chart. Point your mouse over the time axis to determine the average packet loss, as a percentage of the total number of packets sent, measured at that time.
- Jitter chart. Point your mouse over the time axis to determine the average jitter measured at that time, in milliseconds.
- Delay chart. Point your mouse over a bar to determine the average delay measured in that time interval, in milliseconds.
- Echo chart. Point your mouse over the time axis to determine the precise average echo measured at that time, in DB.

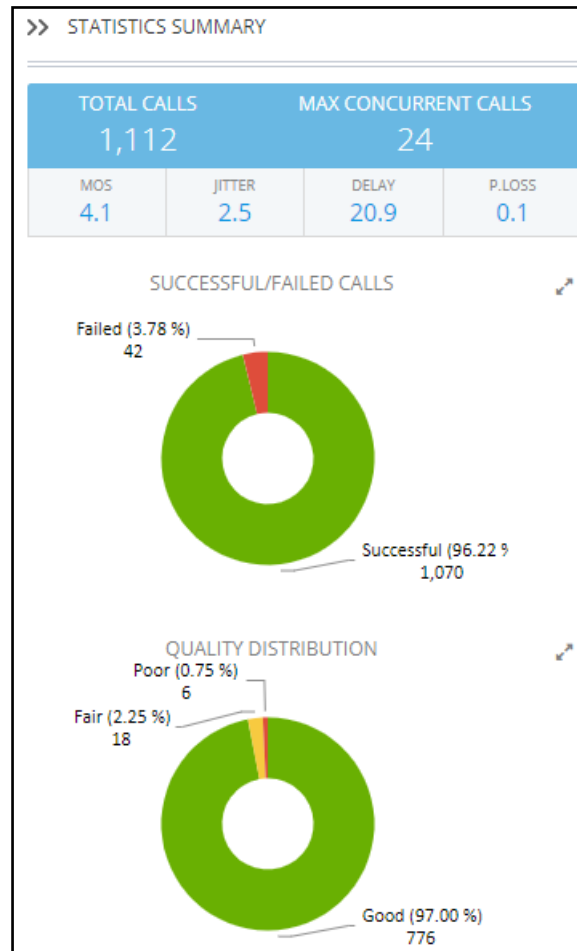


Values displayed in the charts are reported by devices for representation in the OVOC. Sometimes when reported values are higher than expected, for example, packet loss might be higher than 100%, please contact AudioCodes Support for clarification.

## Statistics Summary

On the right side of the Devices Statistics page, you can view the Statistics Summary pane.

**Figure 6-41: Statistics Summary**



The pane displays

- the total # of calls made over devices in the time period
- the maximum concurrent calls measured over devices in the time period
- the values of MOS, Jitter, Delay and Packet Loss quality metrics measured over devices in the time period

The pane also displays two metrics as pie charts:

- Successful/Failed Calls pie chart. Point your mouse over a segment of the color-coded pie chart to determine the # and % of calls that were evaluated as ■ Successful or ■ Failed in that time interval.
- Quality Distribution pie chart. Point your mouse over a segment of the color-coded pie chart to determine the # and % of calls whose voice quality scored ■ Good ■ Fair or ■ Poor in that time interval.

## Viewing Statistics on Streams over Links

The Links tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of streams over links. Information in the page is presented identically to information in the Devices Statistics page, described in [Viewing Statistics on Calls over Devices](#) on page 184). You can optionally filter the page by Time Range (see [Filtering to Access Specific Information](#) on page 147) and Topology (see [Filtering by 'Topology'](#) on page 150).

## Viewing Statistics on Calls over Sites

The Sites tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of calls over sites. Information in the page is presented identically to information in the Devices Statistics page, described in [Viewing Statistics on Calls over Devices](#) on page 184. You can optionally filter the page to display only the information that you require. You can filter by Time Range (see [Filtering to Access Specific Information](#) on page 147) and Topology (see [Filtering by 'Topology'](#) on page 150).

## Viewing Statistics on Calls over Endpoints

The Endpoints tab under the Statistics menu allows you to make a quick assessment of the health of the network from the perspective of calls over endpoints. Information in the page is presented identically to information in the Devices Statistics page, described in [Viewing Statistics on Calls over Devices](#) on page 184). You can optionally filter the page to display only the information that you require. You can filter by Time Range (see [Filtering to Access Specific Information](#) on page 147) and Topology (see [Filtering by 'Topology'](#) on page 150).

## Monitoring Performance

As your network's central management application, the OVOC features Performance Monitoring (PM) capability to help operators make sure the Quality of Service (QoS) purchased by the ITSP | enterprise is delivered to users after it's provisioned. PM metrics are collected from VoIP network devices. The feature allows operators to monitor historical data. Historical data allows for long-term network analysis and planning.



- For a comprehensive list of PM parameters supported on each device, see the *Performance Monitoring Guide*.
- Two OVOC pages (Perf Monitoring | PM Profiles) facilitate efficient and flexible PM setup - see flows below this note.
  - ✓ For information on how to use the Perf Monitoring page, see [Adding a PM Template](#) on the next page.
  - ✓ For information on how to use the PM Profiles page, see [Adding a PM Profile](#) on page 193.

### ➤ To set up PM using the *default PM template*:

1. Open the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**) and make sure it displays a *default* Performance Monitoring (PM) template provided by AudioCodes.
2. Add a new tenant, open the PM Profiles page (**Statistics > PM Profiles**) and make sure the default PM template provided by AudioCodes is *duplicated and displayed as a PM profile*. This profile is automatically attached to every newly added tenant. If other profiles are added, all profiles listed in the page will automatically be attached to every newly added tenant.

### ➤ To set up PM using a *configured PM template*:

1. Open the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**), add a PM template and configure it as default. Optionally, delete the *previous* default (the AudioCodes-provided default PM template will be the first default you'll have). The default PM template, be it the AudioCodes-provided default or a newly configured default, cannot be deleted.

2. Add a new tenant, open the PM Profiles page (**Statistics > PM Profiles**) and make sure the newly configured default template is *duplicated and displayed as a PM profile*; this profile will automatically be attached to every newly added tenant.

➤ **To set up PM per specific device:**

- Open the PM Profiles page (**Statistics > PM Profiles**), add a new PM profile and in its configuration manually attach it to a specific device.

## Adding a PM Template

The OVOC includes an AudioCodes-provided *default* Performance Monitoring (PM) template. Parameters (metrics) selected in the default are those most frequently requested by AudioCodes enterprise and ITSP customers. The OVOC displays the default PM template in the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**).

**Figure 6-42: Perf Monitoring**

PERF MONITORING						
<div> <span>Add</span> <span>Edit</span> <span>Delete</span> <span>Refresh</span> </div>						
CONFIGURATION	DEFAULT	NAME	DESCRIPTION	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL
<div> <div>TEMPLATES</div> <div> SNMP Connectivity  HTTP Connectivity  QoS Thresholds  QoS Status &amp; Alarms  <b>Perf Monitoring</b>  ALARMS  FILE MANAGER  EXTERNAL APPLICATIONS  DEVICE BACKUP </div> </div>	<input checked="" type="checkbox"/>	PM Profile	Factory PM Profile	41	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<div> <div>PERF MONITORING DETAILS</div> <div> <div>DEFAULT</div> <div> NAME: PM Profile  DESCRIPTION: Factory PM Profile  PARAMETERS #: 41  CREATE DATA FILE: <input checked="" type="checkbox"/>  SEND EVENT PER INTERVAL: <input checked="" type="checkbox"/> </div> </div> </div>						



- The default PM template *cannot be deleted*. The **Delete** button is disabled when the default is selected. When selected, the template's details are displayed in the right pane; approximately 40 parameters (metrics) are included in the default.
- If you *add* a PM template and configure the newly added template to be the *default*, the previous will lose its default configuration and you will be able to delete it. Rule: There will always be one default PM template in the Perf Monitoring page, be it the AudioCodes-provided default or a newly added PM template configured as the default.
- The default PM template is *duplicated as a PM profile* in the PM Profiles page (**Statistics > PM Profiles**) shown in the figure following. Every time you add a new tenant, the default PM template together with all other templates (if you configured other templates) are automatically duplicated as profiles in the PM Profiles page, and allocated to that tenant.

**Figure 6-43: PM Profiles**

PM PROFILES						
<div> <span>Add</span> <span>Edit</span> <span>Delete</span> <span>Refresh</span> </div>						
DEFAULT	NAME	DESCRIPTION	TENANT	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL
<input checked="" type="checkbox"/>	PM Profile	Factory PM Profile	MeteorBank	41	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<div> <div>PERF MONITORING DETAILS</div> <div> <div>DEFAULT</div> <div> NAME: PM Profile  DESCRIPTION: Factory PM Profile  TENANT: MeteorBank  PARAMETERS #: 41  CREATE DATA FILE: <input checked="" type="checkbox"/>  SEND EVENT PER INTERVAL: <input checked="" type="checkbox"/>  MANUAL ATTACHMENTS: 0  DEFAULT ATTACHMENTS: 0 </div> </div> </div>						

➤ **To add a PM template:**

1. Open the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**) and click **Add**.

**Figure 6-44: Add PM Template**

**PERFORMANCE MONITORING TEMPLATE**

Name:

Description:

Default: ☐

Create Data File: ☐

Send Event Per Interval: ☐

Parameters (0)

- System (0)
- SBC (0)**
- Gateway (0)
- Network (0)
- IP Group (0)
- Trunk Group (0)
- SRD (0)

☐ Name

☐ Call Stats


	Min	Max	Avg	Val
<input type="checkbox"/> G711 Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> G723 Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> G728 Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> G729a Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> G729e Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> AMR Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> EVRC Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> G729EV Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> EG711 Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> G726 Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> RTA Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> SILK Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/> AMR-WB Active Calls	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	





OK Close

2. Configure the PM template using the table below as reference.

**Table 6-16: PM Template Parameter Descriptions**

Parameter	Description
Name	Enter a name for the template. Choose an intuitive name to facilitate an operator-friendly network management experience later.
Description	Enter a free-text description of the template to help facilitate an operator-friendly network management experience. Example: "This template is for all tenants of Meteor Bank". This can help orient operators when managing complex networks.
Default	The PM Templates page <i>always displays one default</i> PM template. If you select this 'Default' option, the earlier default PM template will lose its default configuration and you'll be able to delete it from the Perf Monitoring page. There will always be a default PM template in the page, be it the AudioCodes-provided default PM template or a newly added operator-configured default PM template. The PM template configured as the default cannot be deleted. Every time you add a tenant, all PM templates listed in the Perf Monitoring page are <i>duplicated as PM profiles</i> in the PM Profiles page ( <b>Statistics &gt; PM Monitoring</b> ) and all PM profiles listed in the PM Profiles page are <i>automatically allocated to that newly added tenant</i> .

Parameter	Description
Create Data File	OVOC's server polls device parameters every 15 minutes and saves the resulting PM metrics in the server's database. Select this option to save the PM metrics (data) <i>as a file</i> in operator-friendly JSON format. All PM information resulting from the poll is conveniently located in this file. An event is sent when the file is created (see the next parameter).
Send Event per Interval	Select this option for an event to be sent every 15 minutes, indicating that all parameters per device were successfully polled. If 10 devices were selected for polling, the event is sent indicating that all parameters on all 10 devices were successfully polled.
Parameters (0)	<p>Indicates how many PM metrics (check boxes) you selected to be polled. (0) indicates that none have been selected (yet). When you select parameters (metrics), the indication changes accordingly. The following tabs are displayed under 'Parameters':</p> <ul style="list-style-type: none"> <li>■ System (0) - Click the tab to select or clear the check box <b>DSP Utilization</b> gauge.</li> <li>■ SBC (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the counter <b>Tel to IP Call Attempts</b> and the gauge <b>Tel to IP Call Duration</b>, and / or the check boxes under 'Other Stats', e.g., <b>Media Legs</b>.</li> <li>■ Gateway (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the <b>G711 Active Calls</b> gauge and the <b>Attempted Calls</b> counter, and / or the check boxes under 'Other Stats', e.g., <b>Media Legs</b>.</li> <li>■ Network (0) - Click the tab to select or clear check boxes under 'Global', for example, the gauge <b>Net Util KBytes Tx</b> and the counter <b>Incoming Discarded Pkts</b>.</li> <li>■ IP Group (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge <b>Invite Dialogs</b> and / or the check boxes under 'Other Stats', e.g., the counter <b>Subscribe Dialogs</b>.</li> <li>■ Trunk Group (0) - Click the tab to select or clear the check box under 'Call Stats', i.e., the gauge <b>Call Duration</b>, the check box under 'Call Failures', i.e., the counter <b>No Resources Calls</b>, and / or the check boxes under 'Trunk Stats', e.g., the counter <b>All Trunks Busy Time</b>.</li> <li>■ SRD (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge <b>ASR</b>.</li> </ul> <p>See the <i>SNMP Reference Guide</i> for detailed information about each PM parameter.</p> <div>  <p>For SBC devices, you can also configure Performance Monitoring parameters for counting the number of call failures for specific SIP responses. These are configured in the SBC device's Web interface's User Defined Failure PM table. For more information, see the SBC device's <i>User's Manual</i>.</p> </div>

Parameter	Description
Metric Name	Select this option to select all check boxes (PM metrics) under all tabs in the Call Stats pane. To include <i>most but not all</i> PM metrics in your template, select 'Name' (all check boxes will be selected) and then clear those to exclude.
Min Max Avg Value [Minimum value, Maximum value and Average value (Avg)],	<p>In the Call Stats pane shown in the next figure, parameters 'Tel-IP Call Attempts' and 'IP-Tel Call Attempts' are <i>counters</i>. A single value (Val) is displayed after they're measured, i.e., # of counted call attempts.</p> <div>  Tel to IP Call Attempts <input type="checkbox"/>  IP to Tel Call Attempts <input type="checkbox"/> </div> <div>  Tel to IP Call Duration [sec] <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>  IP to Tel Call Duration [sec] <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> </div> <p>In the figure, parameters 'Tel-IP Call Duration' and 'IP-Tel Call Duration' are <i>gauges</i>. If all three adjacent check boxes are selected, the # of calls of minimum duration, the # of calls of maximum duration and the # of average-length calls will be monitored.</p>



Thresholds are configured at the SBC level in the device's Web interface, in the Open Device page. See the device's *User's Manual* for more information. Thresholds can alternatively be configured in an ini file and loaded to the device in the OVOC's Software Manager. When a PM parameter value in the device crosses the configured threshold, the device generates an event that is sent to the OVOC.

3. Click **OK** (or **Close** to exit without saving the template).



In the PM Profiles page, operators can manually attach a PM profile to a *specific device within a tenant*. For more information, see [Adding a PM Profile](#) on the next page

### ➤ To view PM templates:

- Open the PM Templates page (**System > Configuration > Templates > Perf Monitoring**).

**Figure 6-45: Performance Monitoring Templates**

PERF MONITORING								
							<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Refresh</a>	
CONFIGURATION <<	DEFAULT	NAME	DESCRIPTION	PARAMETER...	CREATE CSV...	SEND EVENT PER INTER...	>> PERF MONITORING DETAILS	
▲ TEMPLATES SNMP Connectivity HTTP Connectivity QoS Thresholds QoS Status & Alarms <b>Perf Monitoring</b>	✓	PM Profile	Factory PM Profile	42	✕	✕	DEFAULT	✓
	✕	New		17	✕	✕	NAME	PM Profile
	✕	Template		45	✕	✕	DESCRIPTION	Factory PM Profile
	✕	\*New\*		0	✕	✕	PARAMETERS #	42
	✕	new template		3	✕	✕	CREATE CSV FILE	✕
							SEND EVENT PER INTERVAL	✕

### ➤ To view the details of a specific PM template:

- Select the row of the template whose details you want to view, as shown in the preceding figure; the details are displayed in the right pane.

➤ **To edit a PM template:**

1. In the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**), select the template to edit and click **Edit**.
2. In the PM Template page that opens (identical to the page displayed when adding a template), edit the template using the preceding table as reference.

➤ **To delete a PM template:**

- In the Perf Monitoring page (**System > Configuration > Templates > Perf Monitoring**), select the template to delete and click **Delete**.

## Adding a PM Profile

PM templates are *duplicated as PM profiles* in the PM Profiles page (**Statistics > PM Profiles**). Every time you add a new tenant, the default PM template together with all other templates (if you configured other templates) are automatically duplicated as profiles in the PM Profiles page and allocated to that newly added tenant.



You can *manually add a PM profile* in the PM Profiles page and optionally configure it to be the default. If you configure it as the default, the previous default will lose its default configuration and you'll be able to delete it from the page, so there will always be one default PM profile in the PM Profiles page.

➤ **To add a PM profile:**

1. Open the PM Profiles page (**Statistics > PM Profiles**).

PM PROFILES								
<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Refresh</a>								
DEFAULT	NAME	DESCRIPTION	TENANT	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL	>> PERF MONITORING DETAILS	
<input checked="" type="checkbox"/>	PM Profile	Factory PM Profile	MeteorBank	41	✖	✖	DEFAULT <input checked="" type="checkbox"/> NAME <a href="#">PM Profile</a> DESCRIPTION <a href="#">Factory PM Profile</a> TENANT <a href="#">MeteorBank</a> PARAMETERS # <a href="#">41</a> CREATE DATA FILE <a href="#">✖</a> SEND EVENT PER INTERVAL <a href="#">✖</a> MANUAL ATTACHMENTS <a href="#">0</a> DEFAULT ATTACHMENTS <a href="#">0</a>	

2. Click **Add**.

**Figure 6-46: PM Profile**

PERFORMANCE MONITORING PROFILE

Name \*

MeteorBank

Description

PM profile for the SBC located at Meteor Bank, Skyscape City

Parameters (0)

System (0)

SBC (0)

Gateway (0)

Network (0)

IP Group (0)

Trunk Group (0)

SRD (0)

Default

☒

Create Data File

☐

Send Event Per Interval

☐

Tenant \*

MeteorBank

Attachments

Manual 1

Select Devices

Search by name

MeteorBank

SkyscapeCity

devices

SBC 4

Filter

Filters

topic

☐ Name

Min

Max

Avg

Val

☐ System Stats

DSP Util

☐

☐

☐

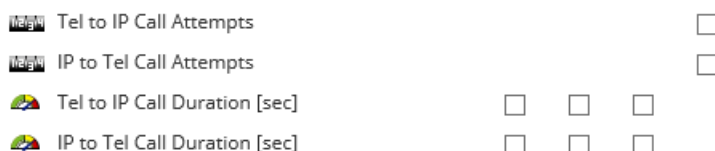
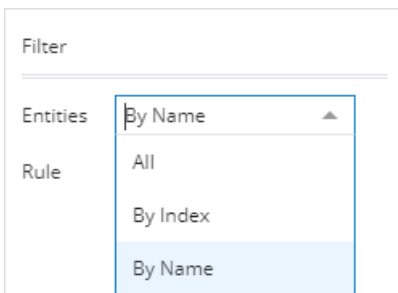
OK

Close

3. Configure a profile using the following table as reference.

**Table 6-17: PM Profile Parameter Descriptions**

Parameter	Description
Name	Enter a name for the profile. Choose an intuitive name to facilitate an operator-friendly network management experience in the future.
Description	Enter a free-text description for the profile to help facilitate an operator-friendly network management experience. Example: This profile is for all tenants in England. The description can help orient operators in complex networks.
Default	The PM Profiles page <i>always displays one default</i> PM profile. If you select this 'Default' option, the previously configured default PM profile - be it the AudioCodes-provided default or a new operator-configured default - will lose its default configuration and you'll be able to delete it from the page. Every time you add a new tenant, the default profile together with all other profiles (if you configured other profiles) are automatically allocated to that tenant.
Create Data File	OVOC's server polls device parameters every 15 minutes and saves the resulting PM metrics in the server's database. Select the option to save the PM metrics (data) as a file in operator-friendly JSON format. All PM information resulting from the poll is conveniently located in this file. An event is sent when the file is created (see the next parameter).
Send Event per Interval	Select this option for an event to be sent every 15 minutes, indicating that all parameters per device were successfully polled. If 10 devices were selected for polling, the event is sent indicating that all parameters on all 10 devices were successfully polled.
Tenant	Select from the drop-down list the tenant to allocate this PM profile to. In the preceding figure, MeteorBank is selected.
Attachments	The <b>Devices</b> link gives operators the option to <i>manually select a specific device</i> to which to attach this PM profile. In the preceding figure, SBC 4 is selected.
Parameters (0)	Indicates how many PM metrics (check boxes) you selected to be polled. (0) indicates that none have been selected (yet). When you select parameters (metrics), the indication changes accordingly. The following tabs are displayed under 'Parameters': <ul style="list-style-type: none"> <li>■ System (0) - Click the tab to select or clear the check box <b>DSP Utilization</b> gauge.</li> <li>■ SBC (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the counter <b>Tel to IP Call Attempts</b> and the gauge <b>Tel to IP Call Duration</b>, and / or the check boxes under 'Other Stats', e.g., <b>Media Legs</b>.</li> <li>■ Gateway (0) - Click the tab to select or clear check boxes under 'Call Stats', e.g., the <b>G711 Active Calls</b> gauge and the <b>Attempted Calls</b> counter, and / or the check boxes under 'Other Stats', e.g., <b>Media Legs</b>.</li> </ul>

Parameter	Description
	<ul style="list-style-type: none"> <li>■ Network (0) - Click the tab to select or clear check boxes under 'Global', for example, the gauge <b>Net Util KBytes Tx</b> and the counter <b>Incoming Discarded Pkts</b>.</li> <li>■ IP Group (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge <b>Invite Dialogs</b> and / or the check boxes under 'Other Stats', e.g., the counter <b>Subscribe Dialogs</b>.</li> <li>■ Trunk Group (0) - Click the tab to select or clear the check box under 'Call Stats', i.e., the gauge <b>Call Duration</b>, the check box under 'Call Failures', i.e., the counter <b>No Resources Calls</b>, and / or the check boxes under 'Trunk Stats', e.g., the counter <b>All Trunks Busy Time</b>.</li> <li>■ SRD (0) - Click the tab to select or clear the check boxes under 'Call Stats', e.g., the gauge <b>ASR</b>.</li> </ul>
Metric Name	Select this option to select all check boxes (PM metrics) under all tabs in the Call Stats pane. To include <i>most but not all</i> PM metrics in your profile, select 'Name' (all check boxes will be selected) and then clear those to exclude.
Min Max Av Value	<p>In the Call Stats pane shown in the figure below, parameters 'Tel-IP Call Attempts' and 'IP-Tel Call Attempts' are <i>counters</i>. A single value (Val) is displayed after they're measured, i.e., the # of counted call attempts.</p>  <p>In the figure, parameters 'Tel-IP Call Duration' and 'IP-Tel Call Duration' are <i>gauges</i>. If all three adjacent check boxes are selected, the # of calls of minimum duration, the # of calls of maximum duration and the # of average-length calls will be monitored.</p>
Filter	<p>Only applies to tabs 'IP Group', 'Trunk Group' and 'SRD'. Enables filtering for specific entities per index or per name. 'Trunk Group' can be filtered only by index.</p> 

Parameter	Description
	For example, after selecting tab 'IP Group' and then selecting <b>By Name</b> , enter a regular expression in the 'Rule' field that is displayed, e.g., <b>^B</b> ; all IP groups whose names begin with <b>B</b> will be polled. The <b>By Index</b> filter enables you to filter specific indexes in the group to be polled; if you enter <b>9</b> (for example) in the 'Rule' field, only row 9 in the IP groups table will be polled (out of a maximum of 5000 indexes supported). This feature allows operators more flexibility when polling for PM.



Thresholds are configured at the SBC level in the device's Web interface, in the Open Device page. See the device's *User's Manual* for more information. Thresholds can alternatively be configured in an ini file and loaded to the device in the OVOC's Software Manager. When a PM parameter value in the device crosses the configured threshold, the device generates an event that is sent to the OVOC.

4. Click **OK** (or **Close** to exit without saving the profile).

➤ **To view PM profiles:**

1. Open the PM Profiles page (**Statistics > PM Profiles**).

**Figure 6-47: PM Profiles**

PM PROFILES								
DEFAULT	NAME	DESCRIPTION	TENANT	PARAMETERS COUNT	CREATE DATA FILE	SEND EVENT PER INTERVAL		
✖	PM Profile	Factory PM Profile	MeteorBank	41	✖	✖		
✔	MeteorBank	PM profile for the SBC located at Meteor Bank, Skyscape City	MeteorBank	31	✖	✖		

>> PERF MONITORING DETAILS	
DEFAULT	✔ MeteorBank
NAME	MeteorBank
DESCRIPTION	PM profile for the SBC located at Meteor Bank, Skyscape City
TENANT	MeteorBank
PARAMETERS #	31
CREATE DATA FILE	✖
SEND EVENT PER INTERVAL	✖
MANUAL ATTACHMENTS	0
DEFAULT ATTACHMENTS	1

2. View the new profile displayed. In the figure, you can see that the new profile 'MeteorBank' was configured as the default profile, replacing the provided default profile 'Factory PM Profile'.

➤ **To edit a PM profile:**

1. In the PM Profiles page (**Statistics > PM Profiles**) select the profile to edit and click **Edit**.
2. Use the preceding table as reference when editing.

## Starting and Stopping PM Polling

The OVOC allows operators to start or stop polling a device (or multiple devices) for Performance Monitoring metrics, in order to decrease the impact PM may have on device resources and to optimize bandwidth consumption.

➤ **To start | stop PM:**

1. Open the Network Topology page (**Network > Topology**) or the **Device Management** page (**Network > Devices > Manage**).
2. Select an entity or multiple entities to poll and then from the 'Actions' drop-down menu, select the **Start Polling** action under the Performance Monitor sub-menu.

**Figure 6-48: Start Polling**

The screenshot shows the 'DEVICE MANAGEMENT' interface. On the left, there's a 'TOPOLOGY' section with a search bar and a list of devices: Zipora2, New, and Tenant12. The main table has columns: NAME, FE, Mediation, IP Address, PRODUCT TYPE, and HA. The 'Actions' menu is open, showing 'MAINTENANCE', 'CONFIGURATION', and 'PERFORMANCE MONITOR'. The 'PERFORMANCE MONITOR' sub-menu is also open, showing 'START POLLING' and 'CHANGE PROFILE'. The table lists three devices with their IP addresses and product types.

NAME	FE	Mediation	IP Address	PRODUCT TYPE	HA
				FE/DB	×
				MEDIAT...	×
172.17.118.51			172.17.118.51	MEDIANT 500 MS...	×
10.3.181.83-9331606			10.3.181.83	MP 1288	×



If a device does not support PM, the Performance Monitor sub-menu in the 'Actions' drop-down menu will not be displayed. It will only be displayed if the selected device or devices support PM.

- After at least 15 minutes (the default polling interval), stop the polling.

**Figure 6-49: Stop Polling**

The screenshot shows the 'DEVICE MANAGEMENT' interface. On the left, there's a 'TOPOLOGY' section with a search bar and a list of devices: Zipora2, New, and Tenant12. The main table has columns: NAME, FE, Mediation, IP Address, PRODUCT TYPE, and HA. The 'Actions' menu is open, showing 'MAINTENANCE', 'CONFIGURATION', and 'PERFORMANCE MONITOR'. The 'PERFORMANCE MONITOR' sub-menu is also open, showing 'STOP POLLING' and 'CHANGE PROFILE'. The table lists three devices with their IP addresses and product types.

NAME	FE	Mediation	IP Address	PRODUCT TYPE	HA
				FE/DB	×
				MEDIAT...	×
172.17.118.51			172.17.118.51	MEDIANT 500 MS...	×
10.3.181.83-9331606			10.3.181.83	MP 1288	×

- View the results of the poll.
  - See [Viewing PM Data Resulting from Polling](#) below

## Viewing PM Data Resulting from Polling

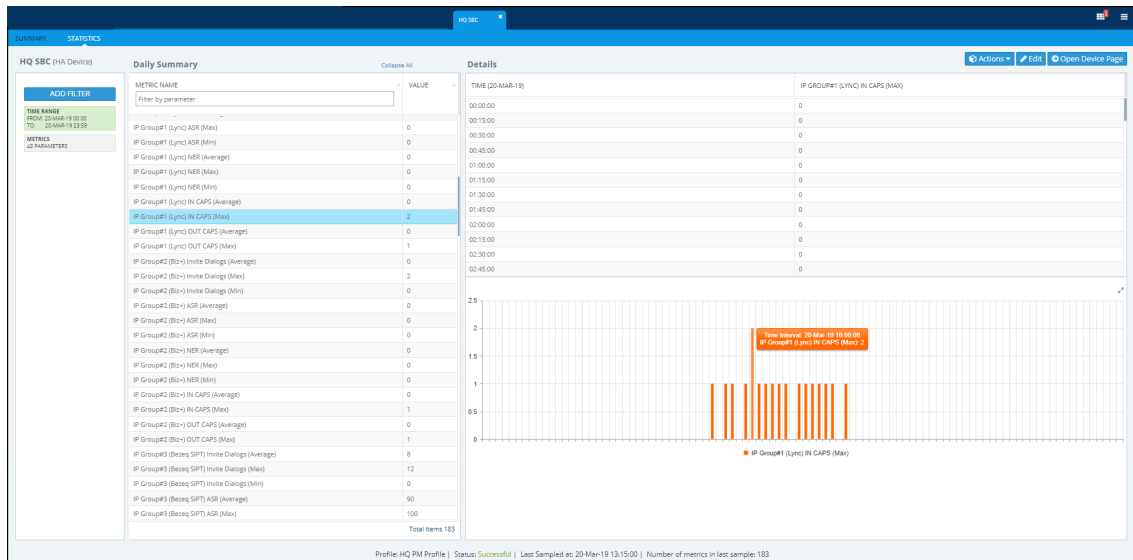
After polling a device (see [Starting and Stopping PM Polling](#) on the previous page), operators can view PM data resulting from polling in:

- the OVOC, in a device's dynamic tab (see [below](#))
- a data file that's created when 'Create Data File' is selected in the PM Profile (see [below](#))
- the OVOC, under Statistics > Devices (see [below](#))

### ➤ To view PM data in a device's dynamic tab:

- Open the Device Management page (**Network > Devices > Manage**), select the device whose PM data you want to view, and then click the **Show** button.
- In the device's dynamic tab's Summary page, click the **Statistics** tab.

Figure 6-50: Device Dynamic tab - Statistics



[Refer to the figure]

- Device Name (HQ SBC) [left side of page]
- ADD FILTER
  - displays the Time Range; click to select a different one; the default is the last 24 hours, 00:00 to 23:59
  - displays the metrics (parameters); click to select fewer, more or different metrics; defaults are taken from this device's PM profile
- Daily Summary - METRIC NAME [middle of page]:
  - the search field 'Filter by parameter' can be used to display (for example) only 'Tel to IP' metrics; all other metrics will be excluded from the list of metric values displayed:

Figure 6-51: Filter by parameter

METRIC NAME	VALUE
tel to ip	
▼ Gateway: 20-Mar-19 (5 Items)	
Tel to IP Call Attempts (Value)	0
Tel to IP Established Calls (Value)	0
Tel to IP Failed Calls due to No Matched Capabilities (Value)	0
Tel to IP Calls Terminated due to a Busy Line (Value)	0
Tel to IP Failed Calls due to Other Reasons (Value)	0

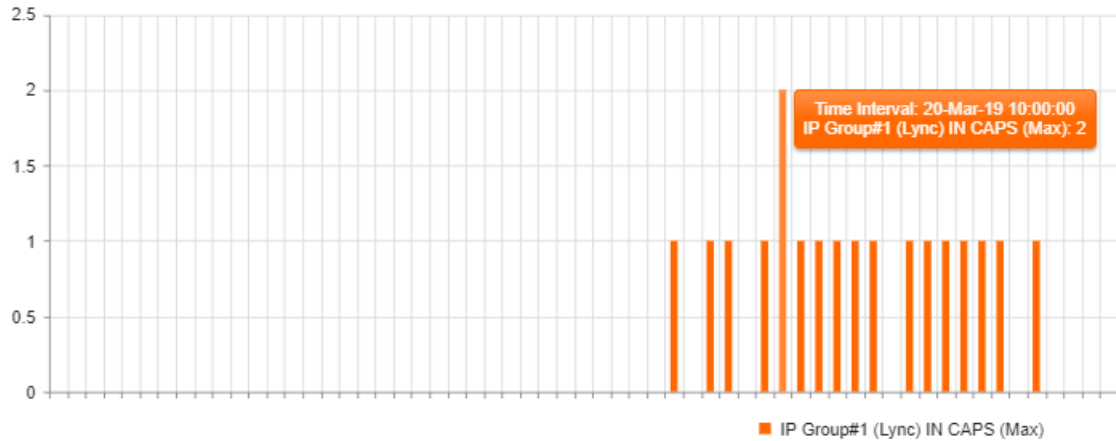
- a summary of metric values measured over the Time Range; the default is 24 hours, from 00:00 to 23:59; the list is structured per entity



Multiple metrics can be selected using the Ctrl key on the keyboard. Operators can select multiple metrics for tabular and graphical comparisons of the metrics.



















- Details [right side of page]:

- after a metric is selected in the Daily Summary list, a table and a bar chart display the distribution details of that metric's values over each 15 minute interval in the Time Range (the default Time Range is 24 hours, from 00:00 to 23:59)
- pointing the cursor over a bar in the chart opens a tool tip summarizing that bar; the tool tip in the figure indicates that the maximum incoming calls per second (CAPS) was measured on IP Group#1 (Lync) in the interval beginning 10:00 on March 20, 2019 to be **2**















- Status bar (lowermost in page):
    - displays the name of the PM profile assigned to the device, the Status of the last polling interval (Successful), the date and time at which the device was last polled, and the number of metrics (parameters) polled in the last interval
- **To view PM data in a data file:**
- Make sure the 'Create Data File' option in the PM Profile is selected. The OVOC's server polls device parameters every 15 minutes and saves the resulting PM metrics in the server's database. If this option is selected, the PM metrics (data) are saved as a file in operator-friendly XML format. All PM information resulting from the poll will conveniently be located in this file. An event is sent when the file is created.
- **To access the data file:**
1. In your browser, enter URL **http://172.17.140.84/nbif** and in the prompt, enter user name **nbif** and password **pass\_1234**.

Figure 6-52: NBIF Index

Index of /nbif			
Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">alarms/</a>	2018-10-21 13:57	-	
 <a href="#">cassandraBackup 7.6...&gt;</a>	2018-11-06 13:17	67M	
 <a href="#">control.ctl</a>	2018-11-06 13:24	9.7M	
 <a href="#">documentation/</a>	2019-01-28 09:20	-	
 <a href="#">emsBackup/</a>	2019-01-30 02:00	-	
 <a href="#">emsServerBackup 7.6...&gt;</a>	2018-11-06 13:21	359M	
 <a href="#">init.ora</a>	2018-11-06 13:23	1.5K	
 <a href="#">ippmanager/</a>	2018-10-25 07:57	-	
 <a href="#">mgBackup/</a>	2019-01-30 04:00	-	
 <a href="#">mibs/</a>	2019-01-28 09:20	-	
 <a href="#">pmFiles/</a>	2019-01-22 13:26	-	
 <a href="#">tmp/</a>	2019-01-28 09:45	-	
 <a href="#">topology/</a>	2019-01-28 09:45	-	
 <a href="#">weekly dbems 06 11 2..&gt;</a>	2018-11-06 13:16	44M	
 <a href="#">weekly dbems 06 11 2..&gt;</a>	2018-11-06 13:21	430M	
 <a href="#">weekly dbems 06 11 2..&gt;</a>	2018-11-06 13:21	1.1M	
 <a href="#">weekly dbems 06 11 2..&gt;</a>	2018-11-06 13:21	1.6M	

2. In the NBIF index, click the entry **pmFiles**.

Figure 6-53: NBIF Index - pmFiles

Index of /nbif/pmFiles			
Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">10.3.181.69-3965360 ..&gt;</a>	2019-01-07 11:31	4.6K	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 11:15	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 11:30	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 11:45	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 12:00	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 12:15	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 12:30	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 12:45	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 13:00	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 13:15	512	
 <a href="#">10.3.181.75 60 2018-..&gt;</a>	2018-11-19 13:30	512	

- File-naming convention:
  - ◆ File Name Format: DeviceName\_Nodetd\_TimeInterval.xml
  - ◆ Time Interval Format: yyyy-MM-dd\_TimeZone\_HH:mm

- ◆ Example: M4K1\_123456\_2018-04-16\_IST\_1200.xml

3. Open the file of the period whose PM metrics you want to view.

**Figure 6-54: Data File Displayed in XML Editor**

```
<?xml version="1.0" encoding="UTF-8"?>
<root>
  <deviceInfo>
    <devicenName>10.3.181.71</devicenName>
    <ip>10.3.181.71</ip>
    <productType>92</productType>
    <sn>5200544</sn>
    <swVersion>7.20A.251.155</swVersion>
    <tenant>
      <tenantName>Zipora</tenantName>
      <region>
        <regionName>Region1</regionName>
      </region>
    </tenant>
  </deviceInfo>
  <timeInterval>
    <from>2019-01-10T06:15:00.000+0000</from>
    <to>2019-01-10T06:30:00.000+0000</to>
  </timeInterval>
  <profile>
    <dictionaryId>1</dictionaryId>
    <id>21</id>
    <name>PM Profile</name>
  </profile>
  <data>
    <topics>
      <topic>
        <parameters>
          <parameter>
            <paramName>
acPMSIPSBAttemptedCallsVal</paramName>
            <parameterData>
              <element>
                <value>0</value>
              </element>
            </parameterData>
          </parameter>
          <parameter>
            <paramName>acPMSBCAsrAverage</paramName>
            <parameterData>
              <element>
                <value>0</value>
              </element>
            </parameterData>
          </parameter>
        </parameters>
        <topicName>SBC</topicName>
      </topic>
    </topics>
  </data>
</root>
```

- XML file format:

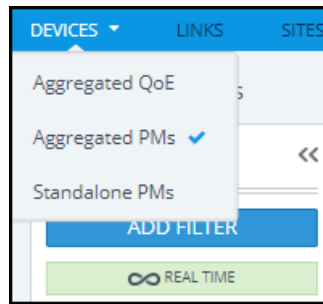
First-Level Info	Second-Level Info	Third-Level Info	Fourth-Level Info
Basic Device Info	Tenant Name	Region Name	-
	Device Name		
	Device IP Address		
	Serial Number (x2 if HA)		
	Product Type		
	Software Version		
Time Period	From Time	-	-
	To Time		
Profile Data	Profile ID	-	-
	Profile Name		
	Dictionary ID		
Polled Data: Structured Polled Data	Topics	Parameter Name	Index:Name:Value

➤ To view aggregated PM metrics from the OVOC's Statistics page:

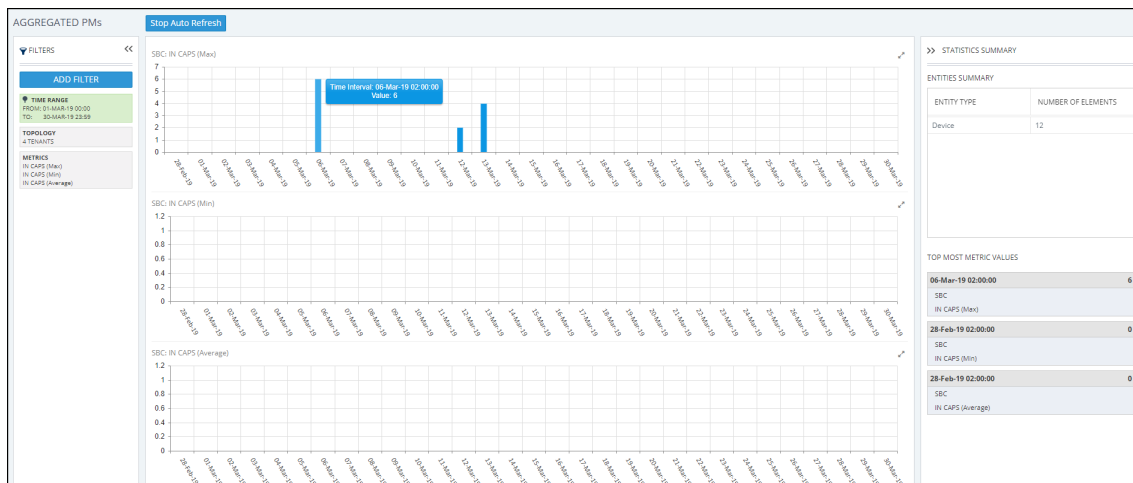


- **Explanation of aggregated PM metrics:** After selecting an aggregated PM metric, the OVOC aggregates it over *all devices and device objects*. For example, after selecting aggregated PM metric X of type 'MIN' measured per IP group over three devices, one graph is displayed; for each timestamp, the OVOC calculates the metric's minimum value over all IP groups over the three selected devices. The metric types are:
  - ✓ MIN – the minimum value measured
  - ✓ MAX – the maximum value measured
  - ✓ AVG – the average value measured
  - ✓ VALUE – summation of values measured
- **Explanation of standalone PM metrics:** Each standalone PM metric is measured and displayed *per specific entity per specific device*. No function is applied.

1. Open the Statistics page and from the **Devices** drop-down, select **Aggregated PMs**.

**Figure 6-55: Selecting 'Aggregated PMs'**

2. In the Aggregated PMs page that opens, you're prompted 'Missing Topology and Metrics Filter'. Click **Add Filter**.
  - a. Change the 'Time Range' or leave it unchanged at the default (the preceding 24 hours, i.e., 00:00 to 23:59).
  - b. Click **Topology** and either select a tenant or multiple tenants, and then click **Apply**.
  - c. Click **Metrics** and select the metrics (parameters) you want to poll. They're displayed like in the PM Profile. Use the information in [Adding a PM Profile](#) on page 193 as reference.
3. View the aggregated PMs then displayed.

**Figure 6-56: Aggregated PMs**

[Refer to the figure]

- **Add Filter (left side of page):**
  - displays the Time Range; click to select a different time range if necessary
  - displays the Topology; click to add, remove or change tenants
  - displays the metrics (parameters); click to select fewer, more or different metrics
- **Bar charts (middle of page):**
  - each chart displays a metric (parameter); scroll down to view all
  - aggregated results are displayed in bars
  - if there are no aggregated results found or if the topmost metric value is 0, no bars are displayed
  - pointing the cursor over a bar displays a tool tip showing the time interval and the metric value
    - ◆ the tool tip in the preceding figure indicates that on this SBC, the maximum aggregated incoming calls per second (CAPS) measured between March 1, 2019 at 00:00 and March 30, 2019 at 23:59, was **6**
- **Statistics Summary (right side of page)**

- 'Entities Summary' displays the entity type | types polled and how many of each type was polled
- Top Most Metric Values indicates the interval in which the highest value was measured for a metric, for example, on 06-Mar-2019 the metric 'IN CAPS (Max)', i.e., the maximum aggregated incoming calls per second (CAPS), was measured to be **6**

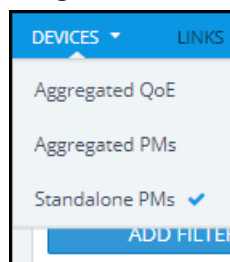
➤ To view standalone PMs from the OVOC's Statistics page:



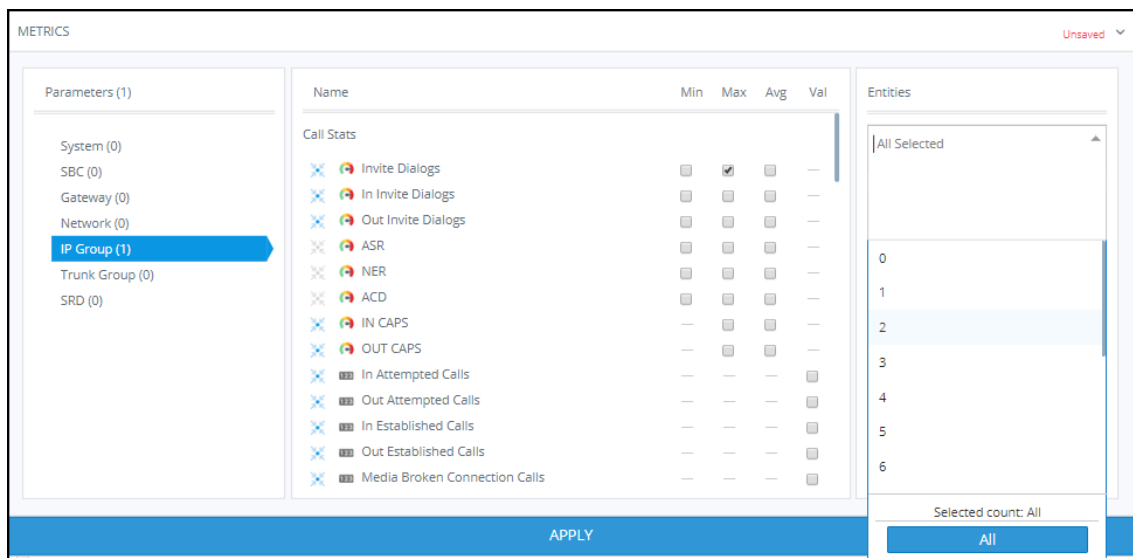
- **Explanation of standalone PM metrics:** Each standalone PM metric is measured and displayed *per specific entity per specific device*. No function is applied.
- **Explanation of aggregated PM metrics:** After selecting an aggregated PM metric, the OVOC aggregates it over *all devices and device objects*. For example, after selecting aggregated PM metric X of type 'MIN' measured per IP group over three devices, one graph is displayed; for each timestamp, the OVOC calculates the metric's minimum value over all IP groups over the three selected devices. The metric types are:
  - ✓ MIN – the minimum value measured
  - ✓ MAX – the maximum value measured
  - ✓ AVG – the average value measured
  - ✓ VALUE – summation of values measured

1. Open the Statistics page and from the **Devices** drop-down, select **Standalone PMs**.

**Figure 6-57: Selecting 'Standalone PMs'**

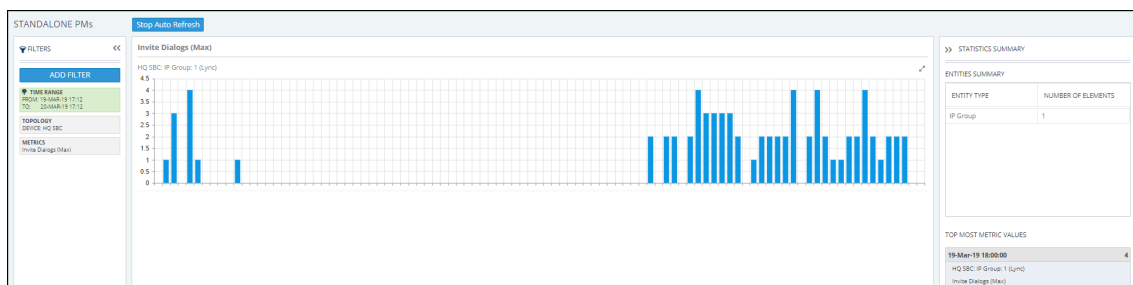


2. In the Standalone PMs page that opens, you're prompted 'Missing Topology and Metrics Filter'. Click **Add Filter**.
  - a. Change the 'Time Range' or leave it unchanged at the default (the preceding 24 hours, i.e., 00:00 to 23:59). Click **Apply**.
  - b. Click **Topology** and select a tenant or multiple tenants and / or a device under a tenant or multiple devices, and then click **Apply**.
  - c. Click **Metrics** and select the standalone PM metrics (parameters) you want to poll. They're displayed in a similar way to the way they're displayed in the PM Profile but for example with the standalone PM metric 'Invite Dialogs' shown in the next figure, Min, Max **or** Av can be selected; you cannot select all three or two, as you can with aggregated PM metrics.
  - d. In the 'Entities' drop-down, select if necessary (and if available) the specific IP Group (for example) to poll. In this case, select its index. You can then select another. Optionally, select **All**.



3. View the standalone PMs metrics then displayed.

**Figure 6-58: Standalone PMs**



[Refer to the figure]

- Add Filter (left side of page):
  - displays the Time Range; click to select a different time range if necessary
  - displays the Topology; click to add, remove or change tenants
  - displays the metrics (parameters); click to select fewer, more or different metrics
- Bar charts (middle of page):
  - each chart displays a metric (parameter); scroll down to view all
  - results are displayed in bars; if there are no results found or if the topmost metric value is 0, no bars are displayed
  - pointing the cursor over a bar displays a tool tip showing the time interval and the standalone PM metric's value
- Statistics Summary (right side of page)
  - 'Entities Summary' displays the entity type | types polled and how many of each type was polled
  - Top Most Metric Values indicates the interval in which the highest value was measured for a metric

## 7 Managing your Network

The OVOC enables ITSPs and enterprises to independently manage their telephony networks.

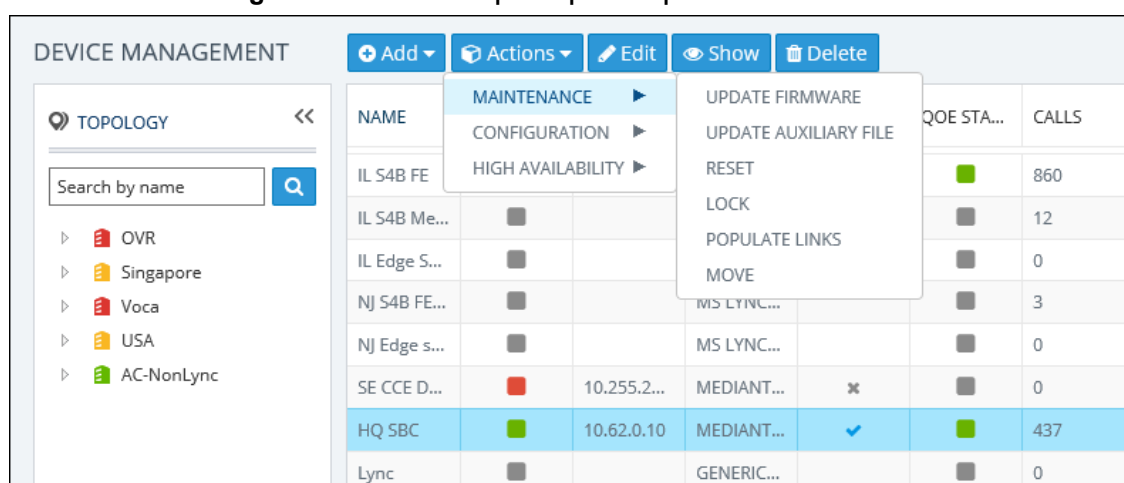
### Performing Management Actions

The OVOC lets operators perform multiple network management actions in the network.

➤ **To perform a management action:**

1. Open the Network page under the **Devices** tab for example.
2. Select a device or a link on which to perform an action; the **Actions** button, **Edit** button, **Show** button and **Delete** button are activated.

**Figure 7-1: Actions | Edit | Show | Delete**



3. Click the **Actions** button and select an action from the drop-down sub-menus.



The sub-menus and the items under them are *dynamic*. They change according to the device selected and its status.

- **Maintenance**
  - ◆ Update Firmware (see [Updating Firmware](#) on the next page)
  - ◆ Update Firmware on Multiple Devices (see [Updating Firmware on Multiple Devices](#) on page 209)
  - ◆ Reset (see [Resetting a Device](#) on page 209)
  - ◆ Lock or Unlock (see [Locking or Unlocking a Device](#) on page 209)
  - ◆ Populate Links (see [Populating Links](#) on page 211)
  - ◆ Move (see [Moving a Device](#) on page 211)
- **Configuration**
  - ◆ Backup (see [Backing Up](#) on page 212)
  - ◆ Restore Last Backup (restore a device's configuration) (see [Restoring the Last Backup](#) on page 213)
  - ◆ Restore Default Configuration (see [Setting Configuration Factory Defaults](#) on page 215)
  - ◆ Save Configuration to Flash (see [Saving a Device's Configuration File to Flash Memory](#) on page 215)

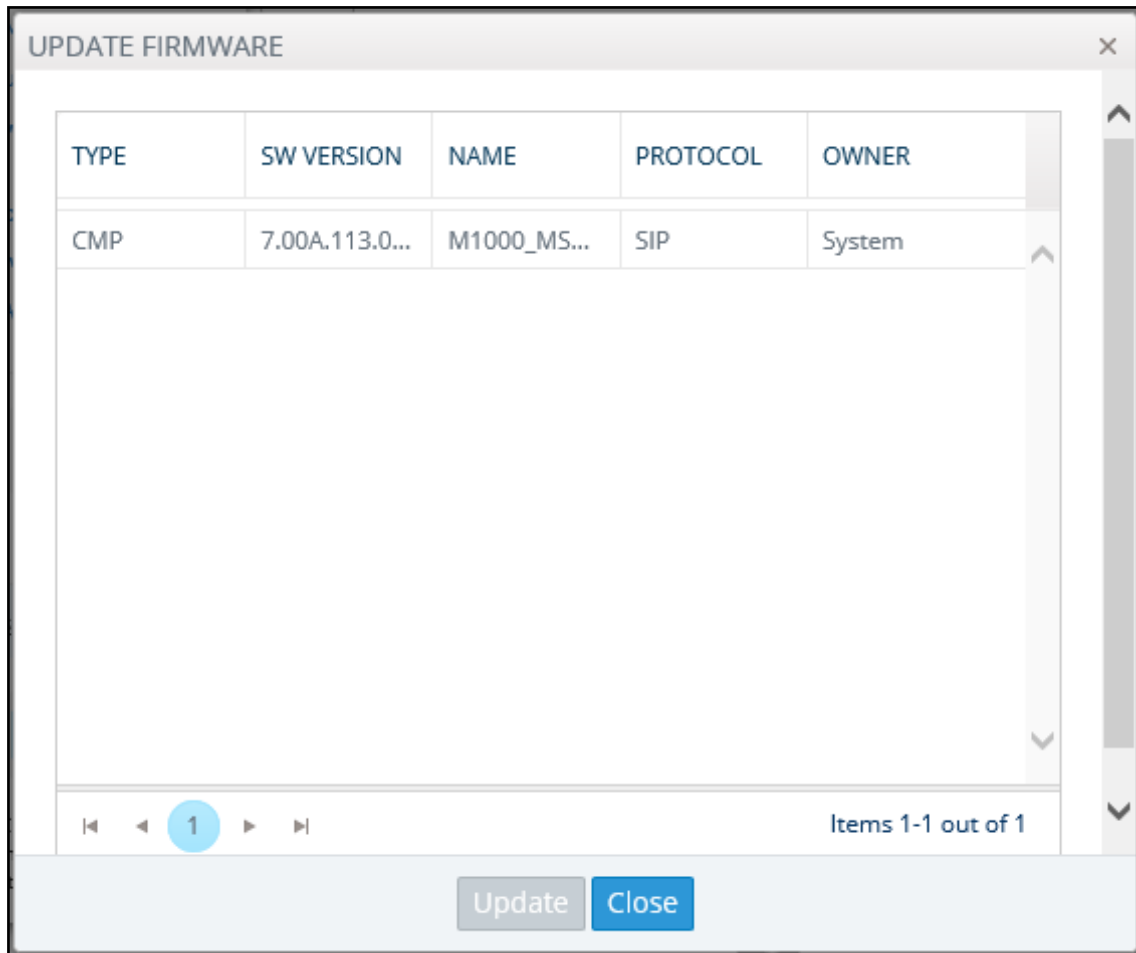
- ◆ Save Current Configuration to File (see [Saving a Device's Configuration File to the PC](#) on page 215)
- **Performance Monitor**
  - ◆ Start Polling (see [Starting Polling](#))
  - ◆ Change Profile (see [Changing Profile](#) on page 217)
- **High Availability**
  - ◆ Reset Redundant (see [Resetting Redundant](#) on page 216)
  - ◆ Switchover (see [Performing Switchover](#) on page 217)
- 4. Use also the following dedicated buttons to perform management actions:
  - **Show** device information (see [Showing Device Information](#) on page 219)
  - **Show** link information (see [Showing Link Information](#) on page 220)
  - **Show** user information (see [Showing User Information](#) on page 221)
  - **Edit** a device (see [Editing a Device](#) on page 223)
  - **Delete** a device (see [Deleting a Device](#) on page 223)

## Updating Firmware

The OVOC lets you update a device's .cmp firmware version file. After loading the .cmp file to the device, you can also load an *ini* file and Auxiliary files (e.g., CPT file).

### ➤ To update a device's firmware:

1. In the Network Topology page, position your cursor over the device.
2. Click **More Actions** and then the **Update Firmware** icon.

**Figure 7-2: Update Firmware**

3. Select the firmware file you require and click **OK**.

## Updating Firmware on Multiple Devices

The OVOC lets you upgrade the .cmp firmware version file on multiple devices. After loading the .cmp file to the devices, you can also load an *ini* file and Auxiliary files (e.g., CPT file).

➤ **To update firmware on multiple devices:**

- In the Network Topology page, select the devices whose firmware you want to upgrade (Ctrl + click devices) and then from the 'Actions' drop-down select **Update Firmware**. Alternatively, in the Device Management page, select the devices whose software you want to upgrade (Ctrl + click devices) and then from the 'Actions' drop-down under the 'Maintenance' sub-menu, select **Update Software**.

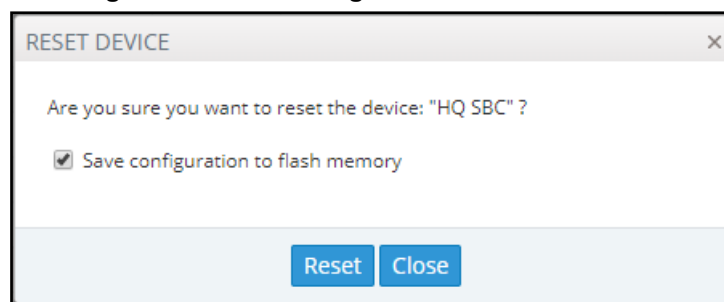
## Resetting a Device

For certain settings to take effect a device reset is required. Resetting a device may also be necessary for maintenance purposes.

➤ **To reset a device:**

1. Open the Device Management page (**Network > Devices > Manage**).
2. Click **Actions** and from the drop-down select **Reset** under the 'Maintenance' menu.

**Figure 7-3: Resetting the Device**



3. [Optional] Select the **Save configuration to flash memory** option.
  - If you select the option, the current configuration will be saved (*burned*) to flash memory prior to reset.
  - If you do not select the option, the device resets without saving the current configuration to flash and all configuration performed after the last configuration save will be discarded (lost) after reset.
4. Click **Reset**.

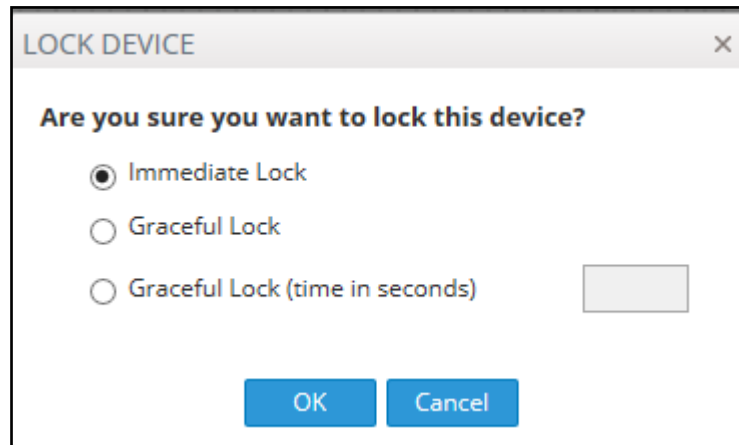
## Locking or Unlocking a Device

Locking a device suspends call functionality and places the device in maintenance state, for troubleshooting, for example. Unlock returns it to service.

➤ **To lock a device:**

1. In the Network Topology page, position your cursor over the device; the Actions menu pops up.
2. Click **More Actions** and then click the **Lock** icon.

Figure 7-4: Lock Device



## 3. Select either:

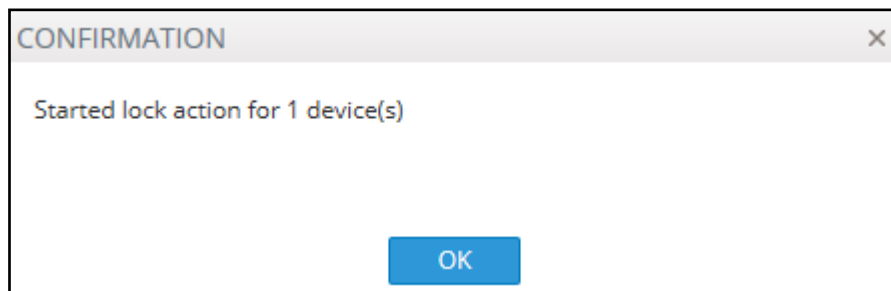
- **Immediate Lock.** The device is locked regardless of traffic. Any existing traffic is terminated immediately.
- **Graceful Lock.** Existing calls first complete and only then is the device locked. No new traffic is accepted.
- **Graceful Lock (time in seconds).** The device is locked only after the time configured in the adjacent field. During this time, no new traffic is accepted. If no traffic exists and the time has not yet expired, the device locks immediately.



These options are available only if the current status of the device is in "UNLOCKED" state

4. Click **OK**.

Figure 7-5: Lock Confirmation



If you selected **Immediate Lock**, the lock process begins immediately. The device does not process any calls.

If you selected **Graceful Lock**, a lock icon is displayed and a window appears displaying the number of remaining (unfinished) calls and time.

➤ **To unlock the device:**

- In the Network Topology page, position your cursor over the device and from the Actions menu shown above, click the **More Actions** link. Click the now-displayed **Unlock** icon; the device unlocks immediately and accepts new incoming calls.

## Populating Links

[See also [Adding Links](#) on page 114] The device action **Populate Links** allows links to be automatically generated and updated between SBCs/gateways and their connected entities. Three different SBC configuration tables are managed by the OVOC:

- IP group
- Trunk group
- Media realm (typically, one for internal (LAN) traffic, another for external (WAN) traffic)

**Populate Links** checks each row in each table and then generates links between AudioCodes devices and generic devices for each row in each table for which a link does not already exist. A new generic device is created for each link.

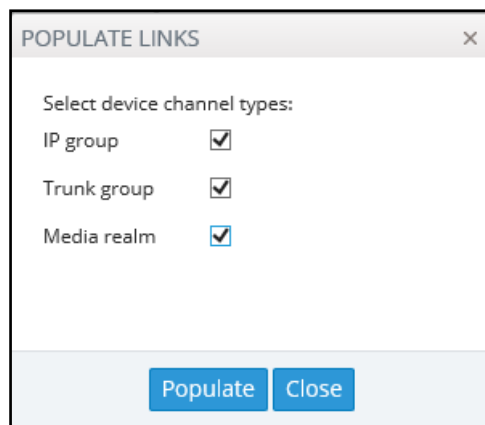
Example:

If two IP Groups, Skype for Business Server 2015 and SIP Trunk ABC, and two Media Realms are configured on an SBC, LAN and WAN, then when **Sync Link** is performed, four links are generated (two IP Groups and two Media Realms).

### ➤ To populate links:

1. In the Network Topology page, position your cursor over the device.
2. Click the **Populate Links** icon.

**Figure 7-6: Populate Links**



3. If necessary, clear an SNMP table option and then click **OK**; links are generated between AudioCodes devices and generic devices for each row in each table where a link does not already exist, and a new generic device is created for each link.

## Moving a Device

The device action **Move** lets you move a device across tenants and/or regions. A device cannot be moved if it has a Zero Touch configuration which has not been applied yet.

### ➤ To move a device:

1. In the Network Topology page, position your cursor over the device; the Actions menu pops up.
2. Click the **Move** icon.

Figure 7-7: Move Device

3. From the 'Tenant' drop-down, select from the list of tenants the tenant to move the device to (see [Adding a Tenant](#) on page 85 for information on how to add a tenant).
4. From the 'Region' drop-down, select from the list of regions the region to move the device to (see [Adding a Region](#) on page 91 for information on how to add a region).
5. If the device is an HA device, configure 'Reset redundant'.
6. Click **OK**.

## Backing Up

You can back up a device's configuration file to the server.

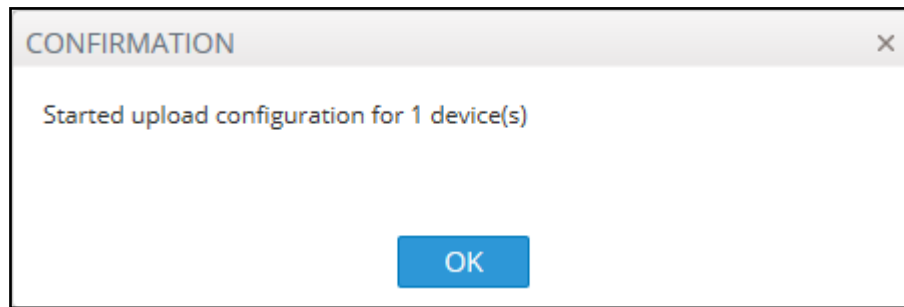
### ➤ To back up a device's configuration file to the server:

1. Open the Device Management page (**Network > Devices > Manage**) and select the device from which to upload the software configuration file to the server.
2. Click **Actions** and from the drop-down choose the 'Configuration' sub-menu.

NAME	MAINTENANCE	BACKUP	QOE S...	CALLS	MAX CO...	QUALITY	SUCCESSFUL...	VERSION	MANAG...	ADMINIST...	LN
SmartTap-10.13.2.11	10.13.2	RESTORE LAST BACKUP		0	0			7.2.100.44		UNLOCKED	
54.22.3.65	54.22.3	RESTORE DEFAULT CONFIGURATION		0	0						
55.55.55.2	55.55.55	SAVE CONFIGURATION TO FLASH		0	0						
10.36.53.2	10.36.53.2	SAVE CURRENT CONFIGURATION TO FILE		0	0						
172.17.140.111	mydevice111	MEDIAN7 8008 E...		0	0			7.20A.240.320		UNLOCKED	
test_device_496073	64.31.35.180	UNLOCKED		0	0						
test_device_6978741	7.7.158.9	UNLOCKED		0	0						
test_device_162271	78.210.13.75	UNLOCKED		0	0						
test_device_422651	183.124.87.85	UNLOCKED		0	0						
test_device_798681	20.240.49.128	UNLOCKED		0	0						
test_device_602206	140.4.115.105	UNLOCKED		0	0						
test_device_598017	191.98.223.94	UNLOCKED		0	0						
test_device_358044	56.253.84.254	UNLOCKED		0	0						
test_device_614011	62.190.247.19	UNLOCKED		0	0						
test_device_894299	87.158.63.227	UNLOCKED		0	0						
test_device_491336	126.144.4.250	UNLOCKED		0	0						
test_device_895005	186.215.143.89	UNLOCKED		0	0						

3. Select the **Backup** option.

4. In the Backup Configuration File prompt, click **Backup**.



- Click **OK**; the latest file is uploaded to the server from the device.



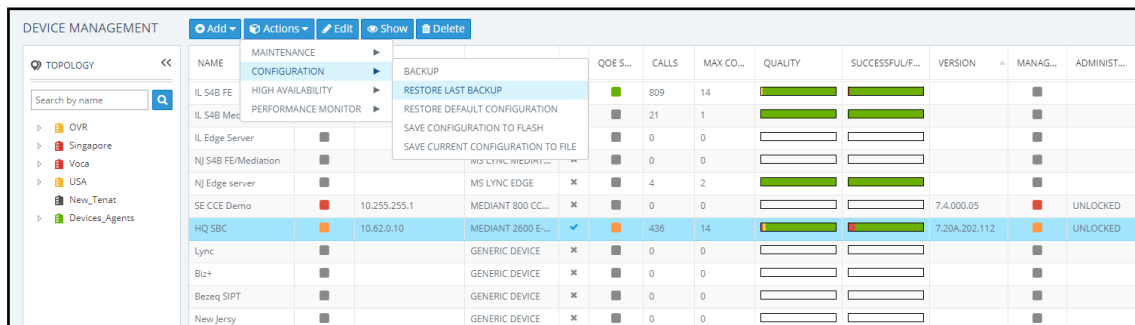
- If the device selected is an MSBR, the latest cli file is uploaded.
- If the device selected is an MP-202 or MP-204, the latest conf file is uploaded.
- If the device selected is any other AudioCodes device (except CloudBond and UMP), the latest ini file is uploaded.

## Restoring the Last Backup

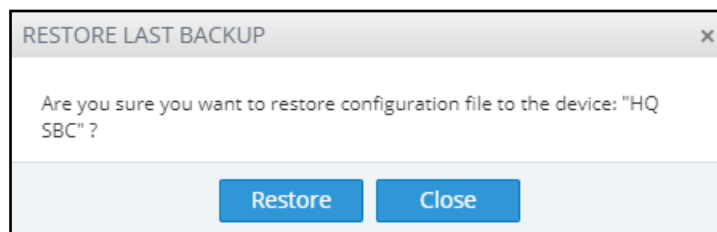
You can restore or download the latest software configuration file, backed up on the server, to the device.

### ➤ To download the latest backup software configuration file to the device:

- Open the Device Management page (**Network > Devices > Manage**) and select the device to which to restore the latest backed-up software configuration file.
- Click **Actions** and from the drop-down choose the 'Configuration' sub-menu.



- Select the **Restore Last Backup** option.



- In the prompt, click **Restore**.
- In the confirmation prompt, click **OK**; the latest file is downloaded to the device from the server.



- If the device selected is an MSBR, the latest cli file is downloaded.
- If the device selected is an MP-202 or MP-204, the latest conf file is downloaded.
- If the device selected is any other AudioCodes device (except CloudBond and UMP), the latest ini file is downloaded.

## Setting Configuration Factory Defaults

You can set a device's configuration to its factory defaults.



The only settings that are not restored to default are the management (OAMP) LAN IP address and the OVOC's login username and password.

## Saving a Device's Configuration File to Flash Memory

You should save (burn) the current configuration of a device to the device's flash memory (non-volatile) before performing a Reset action (see [Resetting a Device](#) on page 209) or before powering down, in order to ensure configuration changes you made are retained.

### ➤ To save (burn) a device's software configuration to the device's flash memory:

1. Open the Devices page (**Network > Devices**) and select the device to which to save (burn) the software configuration.
2. Click **Actions** and select the **Configuration** sub-menu.

**Figure 7-8: Saving Configuration to Flash**

DEVICE MANAGEMENT

Add

Actions

Edit

Show

Delete

TOPOLOGY

Search by name

OVR

Singapore

Voca

USA

New\_Tenat

Devices\_Agents

NAME

CONFIGURATION

HIGH AVAILABILITY

PERFORMANCE MONITOR

IL 54B FE

IL 54B Med

IL Edge Server

NJ 54B FE/Mediation

NJ Edge server

SE CCE Demo

HQ SBC

Lync

Biz+

Bezeq SIPT

MAINTENANCE

CONFIGURATION

HIGH AVAILABILITY

PERFORMANCE MONITOR

BACKUP

RESTORE LAST BACKUP

RESTORE DEFAULT CONFIGURATION

SAVE CONFIGURATION TO FLASH

SAVE CURRENT CONFIGURATION TO FILE

MS LYNC EDGE

MEDIANT 800 CC...

MEDIANT 2600 E...

GENERIC DEVICE

GENERIC DEVICE

GENERIC DEVICE

QOE S...

CALLS

MAX CO...

QUALITY

SUCCESSFULF...

VERSION

MANAG...

ADMINIS...

698

14

17

1

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

0

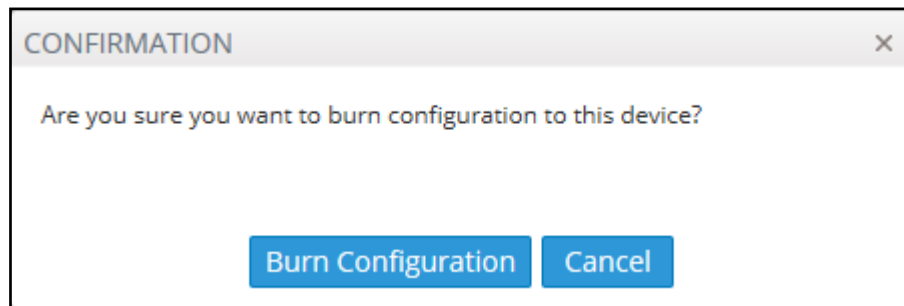
0

0

0

0

3. From the sub-menu, select **Save Configuration to Flash**.



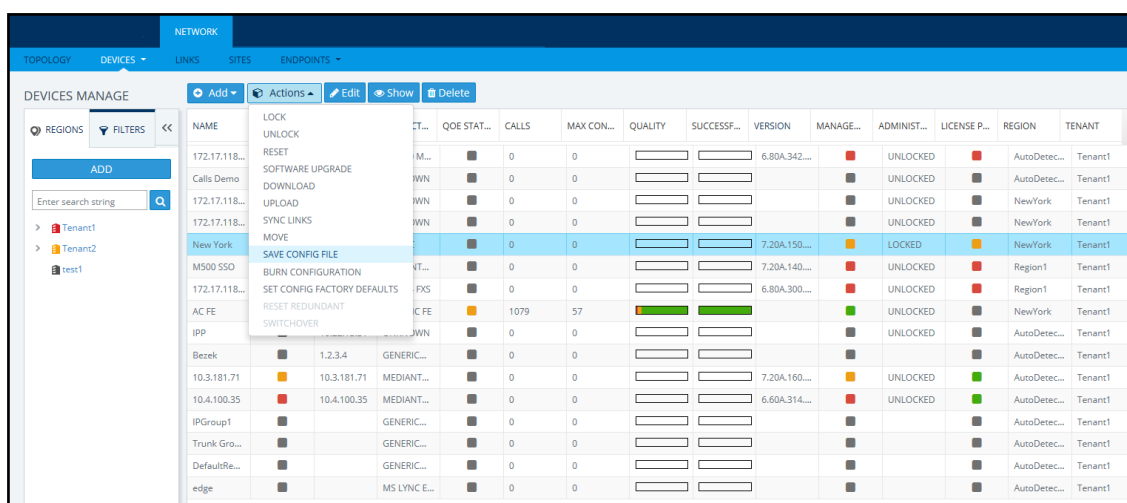
Saving configuration to flash may disrupt current traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (see [Locking or Unlocking a Device](#) on page 209).

## Saving a Device's Configuration File to the PC

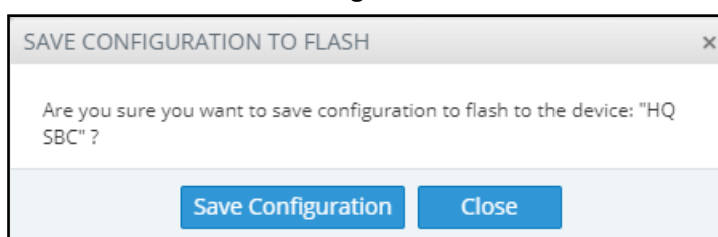
You can save the current configuration of a device to your PC.

### ➤ To save a device's configuration to the PC:

1. Select the device whose configuration you want to save to the PC and click **Actions**.



- From the Actions menu, select **Save Config File**.



- Save the configuration file to the PC's download folder or Save As to the location of your choice.



- If the device is an MSBR, a cli file is saved.
- If the device is an MP-202/MP-204, a conf file is saved.
- If the device is another AudioCodes device (except CloudBond and UMP), an ini file is saved.

## Resetting Redundant

You can reset a device's redundant chassis.

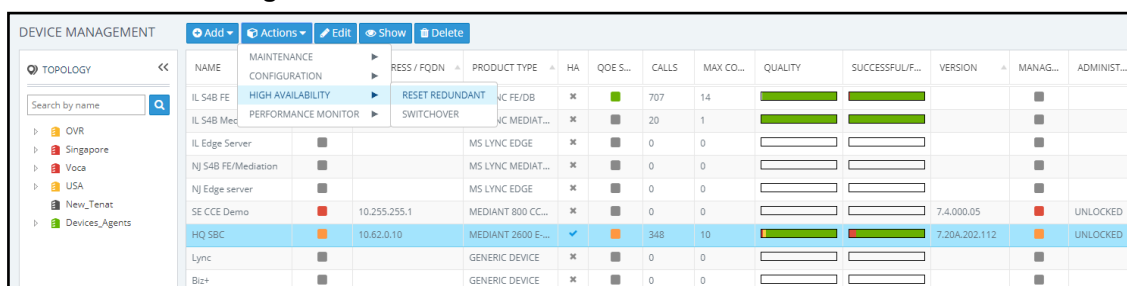


Resetting a device's redundant chassis only applies to HA devices. For detailed information about HA devices, see the relevant device's *User's Manual*.

### ➤ To reset a device's redundant chassis:

- In the Network page under either the **Topology** or **Devices** tab, select the device to reset and then click the now-activated **Actions** button.

**Figure 7-9: Actions – Reset Redundant**



2. From the Actions drop-down, select the **Reset Redundant** option. If the menu option is disabled, the device selected does not support HA.
3. Resetting a device's redundant chassis is identical to resetting an active device. See [Resetting a Device](#) on page 209 for more information.

## Performing Switchover

This only applies to HA devices. For detailed information about HA devices, see the relevant device's *User's Manual*.

If a failure occurs in a device's currently active chassis, a switchover to the redundant chassis occurs. The active chassis becomes redundant and the redundant chassis becomes active. Current calls are maintained and handled by the active chassis (previously the redundant chassis). You can switch from the active chassis (i.e., the previously redundant chassis) to the redundant chassis (i.e., the previously active chassis) to return the device to its original HA state.

### ➤ To perform a switchover:

1. In the Network page under either the **Topology** or **Devices** tab, select the device on which to perform the switchover, and then click the now-activated **Actions** button.

**Figure 7-10: Actions – Switchover**

DEVICE MANAGEMENT													
<div> Add Actions Edit Show Delete </div>													
<div> TOPOLOGY </div>													
<div> NAME MAINTENANCE CONFIGURATION RESS / FQDN PRODUCT TYPE HA QOE S... CALLS MAX CO... QUALITY SUCCESSFUL/F... VERSION MANAG... ADMINIST... </div>													
<div> IL S4B FE HIGH AVAILABILITY RESET REDUNDANT IC FE/DB </div>													
<div> IL S4B Med PERFORMANCE MONITOR SWITCHOVER IC MEDIAT... </div>													
<div> IL Edge Server MS LYNC EDGE </div>													
<div> NJ S4B FE/Mediation MS LYNC MEDIAT... </div>													
<div> NJ Edge server MS LYNC EDGE </div>													
<div> SE CCE Demo 10.255.255.1 MEDIANT 800 CC... </div>													
<div> HQ SBC 10.62.0.10 MEDIANT 2600 E... </div>													
<div> Lync GENERIC DEVICE </div>													
<div> Biz+ GENERIC DEVICE </div>													
<div> Bezeq SIPT GENERIC DEVICE </div>													

2. From the Actions drop-down, select the **Switchover** option. If the menu option is disabled, the device selected does not support HA.

## Changing Profile

Operators can poll a device for Performance Monitoring metrics according to a *PM profile*. For information about defining a PM profile, see [Adding a PM Profile](#) on page 193. A profile determines how the OVOC monitors network | device performance. A profile determines:

- What's monitored [which network | device parameters]
- How frequently [how often they're polled]
- When an alarm is issued [at what parameter threshold]
- Alarm severity [if a parameter threshold is exceeded]

### ➤ To change profile:

1. In the Device Management page (**Network > Devices**), select the **Change Profile** action under the **Performance Monitor** sub-menu in the 'Actions' drop-down menu.

**Figure 7-11: Select PM Profile**

DEVICE MANAGEMENT		Add	Actions	Edit	Show	Delete										
TOPOLOGY	NAME	MAINTENANCE	CONFIGURATION	RESS / FQDN	PRODUCT TYPE	HA	QOE S...	CALLS	MAX CO...	QUALITY	SUCCESSFUL/F...	VERSION	MANAG...	ADMINIST...		
Search by name	IL S4B FE		HIGH AVAILABILITY		MS LYNC FE/DB	✗	695	14								
	IL S4B Mec		PERFORMANCE MONITOR		LYNC MEDIAT...	✗	19	1								
	IL Edge Server				LYNC EDGE	✗	0	0								
	NJ S4B FE/Mediation				MS LYNC MEDIAT...	✗	0	0								
	NJ Edge server				MS LYNC EDGE	✗	0	0								
	SE CCE Demo			10.255.255.1	MEDIANT 800 CC...	✗	0	0				7.4.000.05				
	HQ SBC			10.62.0.10	MEDIANT 2600 E...	✓	345	10				7.20A.202.112				UNLOCKED
	Lync				GENERIC DEVICE	✗	0	0								
	Blz+				GENERIC DEVICE	✗	0	0								

- From the drop-down list, choose the profile (template) according to which to poll the device for PM metrics, and then click **Select**.

SELECT PM PROFILE

Profile

HQ PM Profile

Select

Close

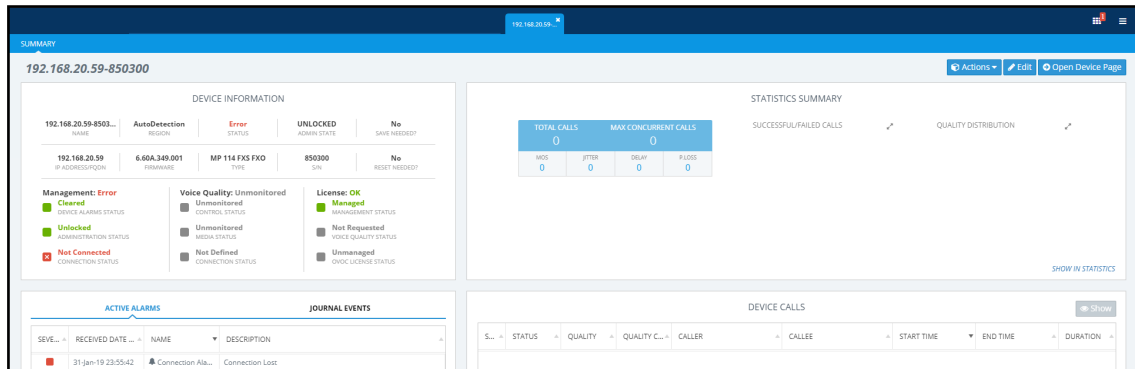
## Showing Device Information

The **Show** button lets operators quickly retrieve and assess information related to any device in the network.

➤ **To show device information:**

1. In the Network page under the **Topology** tab or **Devices > Manage** tab, select the device and click the activated **Show** button.

**Figure 7-12: Show Device Information**




2. The page displays information related to active alarms on the device, journal events, statistics summary and calls made over the device.
3. The page is dynamically automatically tabbed on the menu bar. Operators can delete the tab at any time. The tab facilitates quick future access to the page from other OVOC pages, for troubleshooting.
4. Under the 'Statistics Summary' section of the page, the Successful / Failed Calls pie chart and the Quality Distribution pie chart function as filters. Click a color to open the Calls List filtered by these criteria: Device, Time, Successful / Failed or Quality Color.
5. Under 'Device Calls' you can select a call made over the device and click the **Show** button to display that call's details; the Call Details page opens (see [Showing Call Details](#) on page 232 for more information).

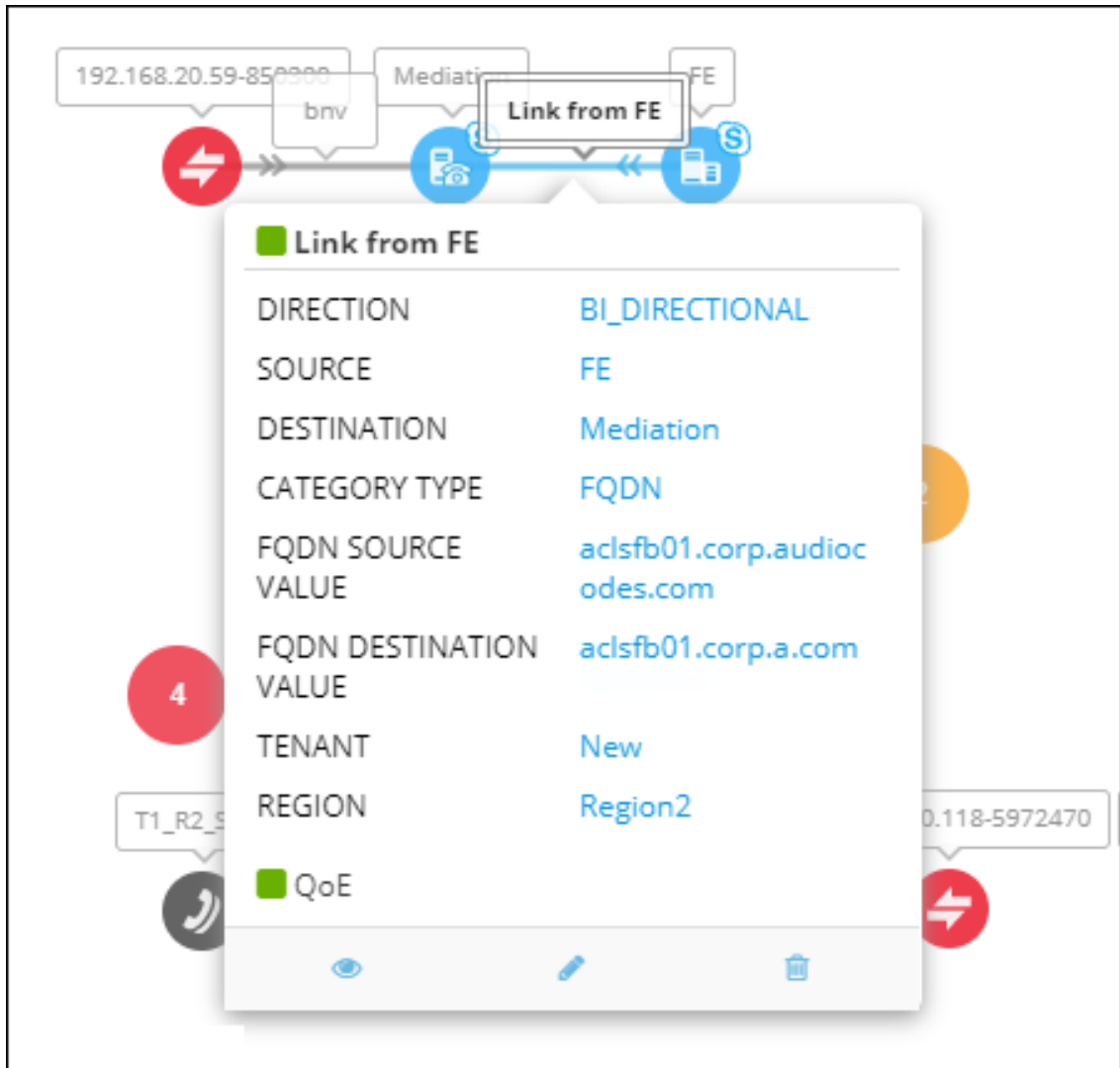
## Showing Link Information

The OVOC lets operators quickly retrieve and assess information related to any link in the network.

➤ **To show link information:**

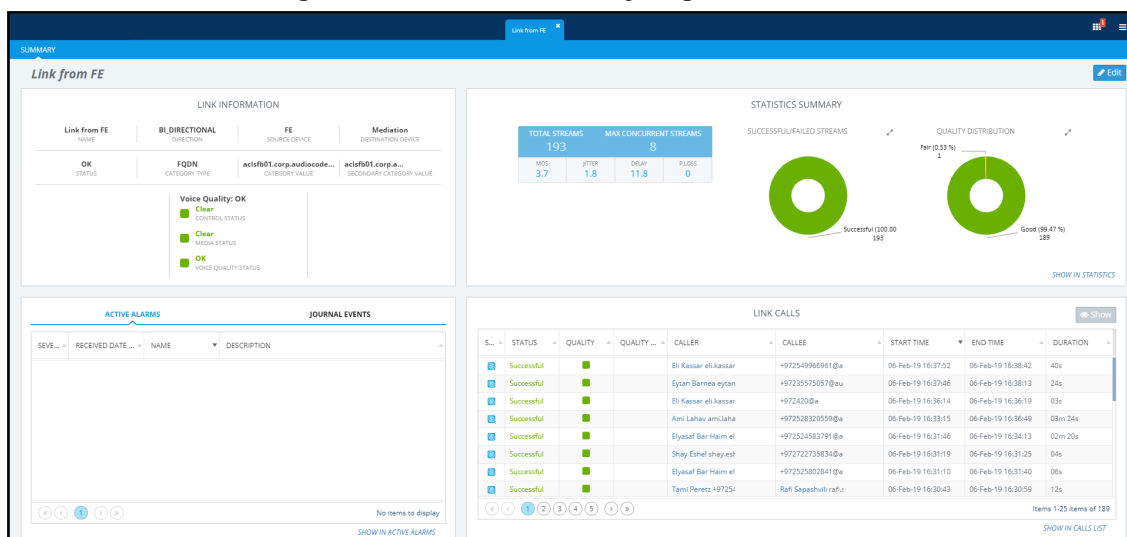
1. In the Network page under the **Topology** or **Links** tab, select the link and click the **Show** button. Alternatively, under the **Topology** tab, hover your mouse device over the link label and from the pop-up menu select the icon .

**Figure 7-13: Show Link Information**



The link's Summary page opens.

Figure 7-14: Link's Summary Page



- The page displays information about active alarms on the link, journal events, statistics summary and calls made over the link.
- The page is dynamically automatically tabbed on the menu bar: **Link from FE** in the figure above. Operators can delete the tab at any time. The tab facilitates quick future access to the page from other OVOC pages, for troubleshooting.
- Under the 'Statistics Summary' section of the page, the Successful / Failed Streams pie chart and the Quality Distribution pie chart function as filters. Click a color to open the Calls List filtered by these criteria: Stream, Time, Successful / Failed or Quality Color.
- Under 'Link Calls' select any call made over the link and click **Show** to display that call's details; the Call Details page opens (see [Showing Call Details](#) on page 232 for more information).

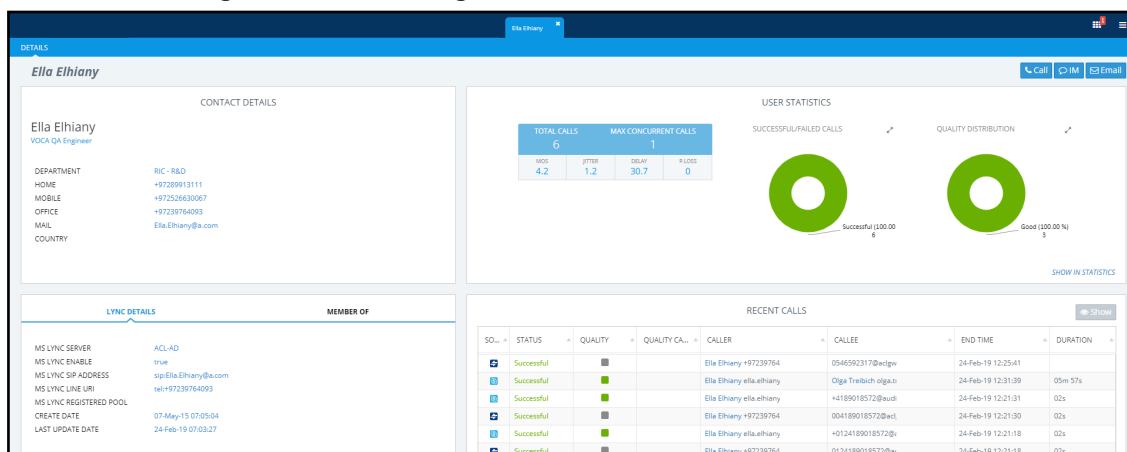
## Showing User Information

The OVOC lets operators quickly retrieve and assess telephony information related to any user.

### ➤ To show telephony information about a user:

- In the Users page under the **Users Experience** or **User Details** tab, select a user and click **Show**.

Figure 7-15: Showing Information about a User



- The page displays contact details, Skype for Business details if any, user statistics and recent calls.

The page is dynamically automatically tabbed on the menu bar with the user's name. Operators can delete it at any time. The tab facilitates quick access to the page from other OVOC pages, for future reference.

3. Under the 'User Statistics' section of the page, the Successful / Failed Calls pie chart and the Quality Distribution pie chart function as filters. Click a color to open the Calls List filtered by these criteria: User, Time, Successful / Failed or Quality Color.
4. Under 'Recent Calls' you can select any call made by this user and then click the **Show** button to display that call's details. The Call Details page opens (see [Showing Call Details](#) on page 232 for more information).

## Editing a Device

The **Edit** button lets you edit a device's configuration.

➤ **To edit a device's configuration:**

1. Select the device to edit and then click the **Edit** button.

**Figure 7-16: Device Details**

AUDIO CODES DEVICE DETAILS

**GENERAL**    SNMP    HTTP    SBA    FIRST CONNECTION

Name: 10.3.181.71

Description: null

Tenant: Tenant1

Region: AutoDetection

☒ IP Address: 10.3.181.71

☐ Serial Number 1: 5200544

Serial Number 2:

OK    Cancel

2. Edit the device's details. For more information, see [Adding AudioCodes Devices Automatically](#) on page 92.
3. Click **OK**.

## Deleting a Device

The **Delete** button lets you delete a device from the OVOC.

➤ **To delete a device:**

- Select the device to delete and then click the **Delete** button.

## Resetting a Device

You can reset a device.

### ➤ To reset a device:

1. In the Device Management page, from the Actions > Maintenance menu, select **Reset**.

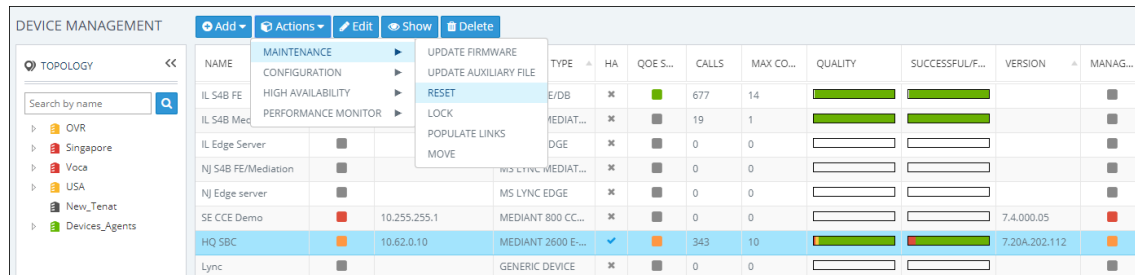
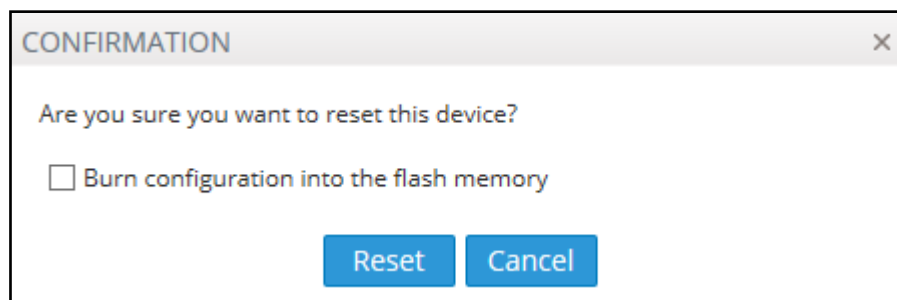


Figure 7-17: Reset Device – Confirmation



2. Select the **Burn configuration into the flash memory** in order to make sure changes are retained. They're burned (saved) to the device's non-volatile memory, i.e., flash memory. See [Saving a Device's Configuration File to Flash Memory](#) on page 215 for more information about burning a device's configuration to flash memory.



Without burning, changes are saved to the device's *volatile* memory (RAM). The changes revert to their previous settings if the device subsequently resets (hardware or software) or powers down.

3. Click **Reset**.

## Refreshing a Device's Pool License

You can refresh a device's Pool License.



Only relevant to HA devices. A switchover is performed in order to apply the license parameter on both devices.

➤ **To refresh a device's Pool License:**

- From the Actions menu, select **Refresh License**.

## Monitoring Device-Level Backup and Performing Rollback

The Backup Manager page (**Network** > **Devices** drop-down > **Backup Manager**) allows you to monitor device-level backup and perform rollback. For detailed information, see [Backing up a Device's Configuration using Backup Manager](#) on page 112.

## 8 Obtaining Quality Statistics on Calls

You can get quality statistics a.k.a. Key Quality Indicators (KQIs) on calls made by end users in your telephony network.

### Accessing the Calls List

The Calls List page (**Calls > Calls List**) lists and shows quality information on calls made in the network over the past three hours (default).

**Figure 8-1: Calls List**

CALLS LIST												
CALLS LIST												
SOURCE	STATUS	QUALITY	QUALITY CA...	CALLER	CALLER	START TIME	END TIME	DURATION	CALL TYPE	DEVICE	LINK	TERMINATION R...
Successful				Yanir Gansburg +97239764	0526406223@edgw01.corp	24-Feb-19 16:10:34	24-Feb-19 16:11:31	48s	SBC	HQ SBC	Lync ARM	Normal Call Clear
Successful				Pavel Smolyar +972397643	0545249114@edgw01.corp	24-Feb-19 16:10:09	24-Feb-19 16:10:19		SBC	HQ SBC	Lync ARM	Normal Call Clear
Successful				Lior Ratz +97239764412@i	00433848@edgw01.corp.auc	24-Feb-19 16:09:54	24-Feb-19 16:09:55	01s	SBC	HQ SBC	Lync ARM	Normal Call Clear
Successful				Vladimir Sheinkerman +97	0528275004@edgw01.corp	24-Feb-19 16:09:43	24-Feb-19 16:09:43		SBC	HQ SBC	Lync ARM	Normal Call Clear
Successful				Itai Rozen +97239764751@	0462@edgw01.corp.audloo	24-Feb-19 16:09:01	24-Feb-19 16:09:05	04s	SBC	HQ SBC	Lync ARM	Normal Call Clear
Successful				(544384103@10.9.9.5	Sharon Ofir +97239764189@	24-Feb-19 16:07:55	24-Feb-19 16:08:26	05s	SBC	HQ SBC	Bezeq SIP, L...	Normal Call Clear
Successful				Jonathan Reberger +972397	0542095956@edgw01.corp	24-Feb-19 16:07:27	24-Feb-19 16:07:46	10s	SBC	HQ SBC	Lync ARM	Normal Call Clear
Successful				(526406223@10.9.9.5	Yanir Gansburg +97239764	24-Feb-19 16:06:03	24-Feb-19 16:06:23		SBC	HQ SBC	Bezeq SIP, L...	Normal Call Clear
Successful				SIXT +97239764145@audioc	0544539417@edgw01.corp	24-Feb-19 16:05:21	24-Feb-19 16:06:05	35s	SBC	HQ SBC	Lync ARM	Normal Call Clear






Calls on AudioCodes High Availability devices during switchover are not supported. The OVOC QoE application does not display and count a call that starts on unit A and is transferred to unit B after device switchover.

The page features filtering capabilities to help obtain precise information on calls quickly and efficiently. Optionally, filter the page by Time Range (see [Filtering to Access Specific Information](#) on page 147), Topology (see [Filtering by 'Topology'](#) on page 150), Source Type (see [Filtering by 'Severity'](#) on page 158), Quality (see [Filtering by 'Quality'](#) on page 228) or More Filters (see [Filtering by 'More Filters'](#) on page 230).

Use the following table as reference to the columns in the Calls List.

**Table 8-1: Calls List Columns**

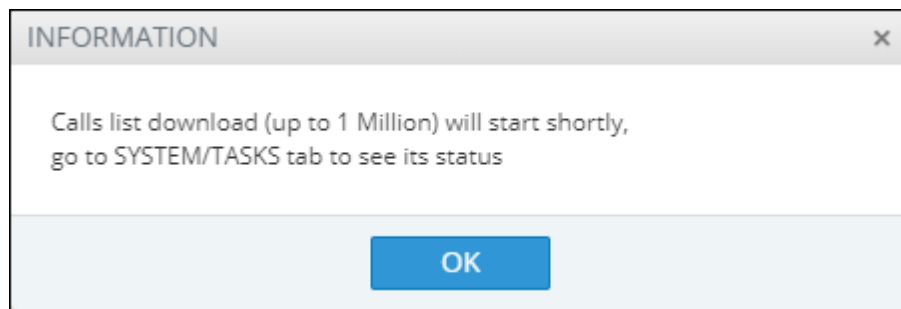
Column	Description
Source	 indicates the call is from Microsoft Skype for Business  indicates the call is from an AudioCodes device.  indicates the call is from an AudioCodes IP phone.
Status	Indicates call control status: <b>Successful</b> or <b>Failed</b>
Quality	Indicates the call quality: Green = Good, Yellow = Fair, Red = Poor, Gray = Unknown

Column	Description	
Quality Cause	Delay (msec)	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter (msec)	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss (%)	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
Caller	The phone number or address of the person who initiated the call.	
Callee	The phone number or address of the person who answered the call.	
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was started.	
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.	
Duration (sec)	The duration of the call, in seconds. See the note following.	
Call Type	Indicates the call type.	
Device	Indicates the device/s over which the call passed.	
Link	Indicates the link/s over which the call passed.	
Termination Reason	Indicates the reason why the call was terminated.	



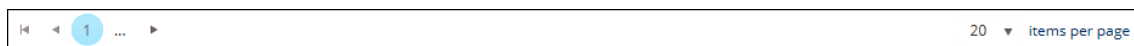
An SBC call (exclusively) whose duration is longer than three hours (e.g., the session of a participant in a Skype for Business conference call over an SBC) or an SBC call that is incompletely reported to the OVOC server won't be displayed in the Calls List.

The **Save** button allows operators to save up to one million calls to a zip file comprising 10 separate csv files, each including up to 100,000 calls.



A README file is also included in the save, with details of the Calls List filter settings, the number of exported entities, the time range and the tenant operator credentials.

The foot of the page features a pager.



The pager lets you (from left to right):

- Click the |◀ **Go to the first page** to return to the first page from any page.
- Click the **Go to the previous page** arrow to return to the page before the presently displayed page.
- Click ... **[More pages]** to the left of the page number or ... **[More pages]** to the right of the page number to page backwards or forwards respectively.
- Click the **Go to the next page** arrow to browse to the page after the presently displayed page.
- From the 'Items per page' drop-down, select the number of calls to display per page: **20, 30 or 50.**

## Filtering by 'Quality'

You can filter a page using the 'Quality' filter. The filter applies to the Calls List page under the Calls menu. The filter lets you display calls according to quality.

**Figure 8-2: Quality Filter**

TIME RANGE >

TOPOLOGY >

SOURCE TYPE >

QUALITY ▾

**Status:**

☒ Failed

☒ Success

**Quality:**

☒ Poor

☒ Fair

☒ Good

☒ Unknown

**Cause:**

☒ None

☒ MOS

☒ Jitter

☒ Delay

☒ P. Loss

☒ Echo

MORE FILTERS >

APPLY

Use the following table as reference.

**Table 8-2: 'Quality' Filter**

Filter	Description
Failed   Success	Filters calls according to their status. If you clear Success and select Failed, only calls whose status was Failed are displayed in the page.
Poor, Fair, Good or Unknown	Filters calls according to their quality. If you clear all except Poor, only calls whose quality was Poor will be displayed.
None, MOS, Jitter, Delay, P. Loss or Echo	Filters calls according to the cause of the quality. If - after displaying only calls whose quality was poor/fair - you clear all except Delay, the page will display only calls <i>whose quality was poor/fair because there was a delay on the line</i> .

## Filtering by 'More Filters'

The Calls List page can be filtered using the 'More Filters' filter. This filter lets you display calls according to caller, callee, media type, etc.

**Figure 8-3: More Filters – Calls List Page**

The screenshot shows a mobile interface for filtering calls. At the top, there are five filter categories: TIME RANGE, TOPOLOGY, SOURCE TYPE, QUALITY, and MORE FILTERS. Each category has a right-pointing chevron. The MORE FILTERS category is expanded, showing a list of filters: Caller, Callee, Media Type, and Call Type. Each filter has a text input field and a downward-pointing chevron. At the bottom of the expanded section is a grey button labeled APPLY.

Use the following table as reference.

**Table 8-3: More Filters – Calls List**

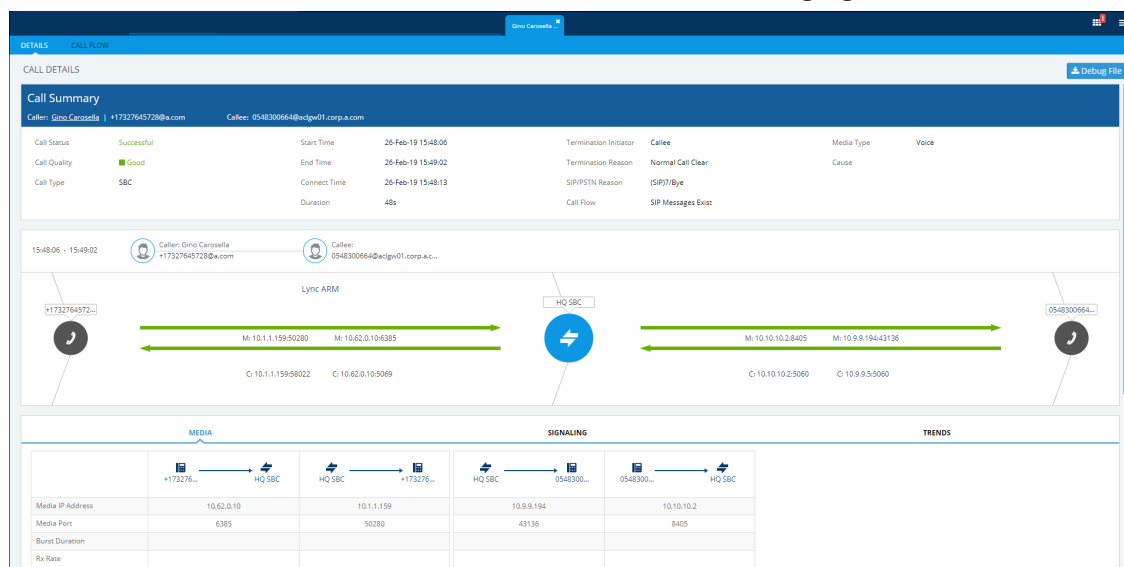
Filter	Description
Caller	Enter the name of a caller (or the names of callers) whose calls you want to display in the page. The filter is case sensitive.
Callee	Enter the name of a called party (or the names of called parties) whose calls you want to display in the page. The filter is case sensitive.

Filter	Description
Media Type	From the drop-down list, select the media type to display on the page (or enter a search string). Select either MSRP (Message Session Relay Protocol), Voice, Image, Application Sharing (a Skype for Business media type), Video, Data, Audio Video, Chat, Audio V150 (currently unsupported), Text, Unknown or All (and then optionally remove unwanted media types). By default, all media types are selected.
Call Type	<p>From the drop-down list, select the call type to display on the page, or enter a search string. Select either GW (Gateway), SBC, Skype Conference, Endpoint, Test SBC, HTTP, IP2IP or Skype.</p> <p>Skype Conference can be of media type 'Audio Video' or 'Chat'. The conference participant's name is shown in the 'Caller' column. To retrieve conference calls information, the OVOC uses the Microsoft Skype for Business ConferenceSessionDetailsView Monitoring Server report. For example, from the 'Media Type' drop-down choose Chat; the Media Type column then displays only MS Skype for Business conferences whose Media Type is Chat.</p>
Termination Reason	<p>Enter the reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.</p> <p>Some AudioCodes termination reasons are:</p> <ul style="list-style-type: none"> <li>■ Reason Not Relevant</li> <li>■ Unassigned Number</li> <li>■ Invalid Information Element Content</li> <li>■ The remote equipment received an unexpected message that does not correspond to the current state of the connection.</li> <li>■ Recovery on Timer Expiry</li> <li>■ Protocol Error Unspecified</li> <li>■ Unknown Error</li> <li>■ Q931 Last Reason</li> </ul> <p>Some MS Skype for Business Termination Reasons are:</p> <ul style="list-style-type: none"> <li>■ OK. Indicates the request was successful.</li> <li>■ Accepted. Indicates that the request has been accepted for processing, but the processing has not been completed.</li> <li>■ No Notification</li> <li>■ Multiple Choices</li> <li>■ Moved Permanently</li> <li>■ Moved Temporarily</li> <li>■ Use Proxy</li> <li>■ Alternative Service</li> </ul>

## Showing Call Details

After filtering the calls listed in the Calls List page by either Time Range (see [Filtering to Access Specific Information](#) on page 147), Topology (see [Filtering by 'Topology'](#) on page 150), Source Type (see [Filtering by 'Severity'](#) on page 158), Quality (see [Filtering by 'Quality'](#) on page 228) and / or More Filters (see [Filtering by 'More Filters'](#) on page 230), select the call whose details you want to view and then click the activated **Show** button. The Call Details page that opens displays detailed information about that call.

**Figure 8-4: Call Details – Details of a Call Made over a Device Belonging to AudioCodes**



## Details of a Call Made over an AudioCodes SBC

The figure above shows the details of a call made over the AudioCodes SBC. You can also display the details of calls made/received over other entities. The page is automatically dynamically tabbed on the menu bar for quick and easy future access and troubleshooting. Operators can delete the tab at any time. The page displays detailed diagnostic information, in graphic and textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality. Use the following table as reference.

**Table 8-4: Call Details Page**

Page Sub-division	Description
(Uppermost) Call summary	Displays parameters and values identical to those displayed in the Calls List page.
(Middle) Graphic illustration	<p>Displays a graphical illustration of voice quality on each leg of the call, on both the caller and callee side. Each leg is:</p> <ul style="list-style-type: none"> <li>Connected via the VoIP cloud to the device</li> <li>Color-coded to indicate quality (green = good, yellow = fair, red = poor, grey = unknown)</li> <li>Tagged by C and M <ul style="list-style-type: none"> <li>C = Control summary (point cursor to view tooltip)</li> <li>M = Media IP address and Port (point cursor to view tooltip)</li> </ul> </li> </ul>

Page Sub-division	Description
(Lowermost) Three tabs	<p>Each opens a page displaying detailed information:</p> <ul style="list-style-type: none"> <li>Media (see <a href="#">Media</a> below) (includes Quality)</li> <li>Signaling (see <a href="#">Signaling</a> on page 236)</li> <li>Trend (see <a href="#">Trends</a> on page 237) (Only displayed if there is a trend; if there is not a trend, the tab is not displayed)</li> <li>SIP Ladder (see <a href="#">SIP Call Flow</a> on page 238)</li> </ul>

## Media

The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

**Figure 8-5: Media**

CALL DETAILS									
	MEDIA				SIGNALLING				TRENDS
	+972397...	E-SBC	E-SBC	+972397...	E-SBC	123@AC...	123@AC...	E-SBC	
Media IP Address	10.1.1.158		10.62.0.10		10.10.10.2		10.9.9.130		
Media Port	51592		6920		8990		42582		
Signal Level									
Noise Level									
SNR									
Burst Duration									
Rx Rate	87		0		87		87		
Quality	GOOD		GOOD		GOOD		GOOD		
MOS			4.1		4.1				
Jitter	1		6		5		2		
Packet Loss									
Delay			3						
Echo									
Media IF		MRLAN				MRWAN			
Network IF		Voice				WANSP			
Coder		G711Mulaw				G711Alaw_64			
SCE		false				false			
RTP Direction		Send Receive				Send Receive			
RTCP Direction		Send Receive				Send Receive			
P-Time		20				20			

Use the following table as reference to the parameters displayed under the Media tab.

**Table 8-5: Media Parameters**

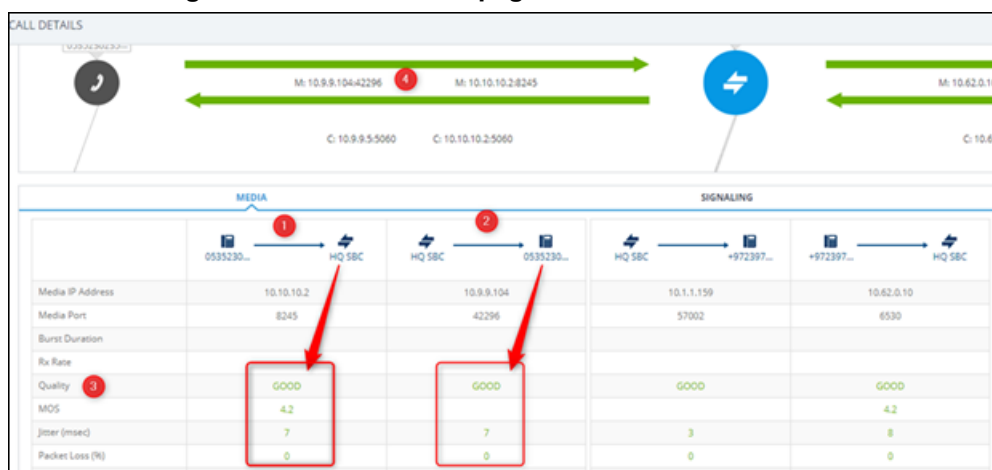
Parameter	Description
Media IP Address	<ul style="list-style-type: none"> <li>The IP address of the device source in the operations, administration, and provisioning (OAMP) network.</li> <li>The IP address of the destination host / media network.</li> </ul>
Media Port	<ul style="list-style-type: none"> <li>The device's source port in the operations, administration, and provisioning (OAMP) network.</li> <li>Port of the destination host / media network.</li> </ul>
Signal Level	<p>The ratio of the voice signal level to a 0 dBm0 reference. Signal level = 10 Log10 (RMS talk spurt power (mW)). A value of 127 indicates that this parameter is unavailable.</p>
Noise Level	<p>The ratio of the level of silent-period background noise level to a 0 dBm0 reference. Noise level = 10 Log10 (Power Level (RMS), in mW, during periods of silence). A value of 127 indicates that this parameter is unavailable.</p>

Parameter	Description
SNR	The ratio of the signal level to the noise level (Signal-Noise Ratio). SNR = Signal level – Noise level.
Burst Duration	The mean duration (in milliseconds), of the burst periods that have occurred since the initial call reception.
Rx Rate	Shows the call's reception rate, in Kbps.
Quality	Voice quality: Good (green), Fair (yellow) OR Red (poor).
MOS	Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises: MOS-LQ = listening quality, i.e., the quality of audio for listening purposes. Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg. MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.
Jitter	Jitter can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
Packet Loss	Lost packets are RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, for the caller and for the callee side. Packet Loss can be more than 100%.
Delay	The round trip delay is the estimated time (in milliseconds) that it takes to transmit a packet between two RTP stations. Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two values are shown, one caller side and another for the callee side.
Echo	The residual echo return loss is the level difference (measured in dB) between the signal transmitted to the listener and the residual echo of that signal.
Media IF	Shows the name and index of the Media Realm interface reported by the device. Example: <b>SIMcmxLAN (n)</b> , where <b>n</b> following the displayed name is the number indicating the Media Interface's index used to facilitate network configuration.
Network IF	Network Interface Name.
Coder	Up to 10 coders (per group) are supported. See the device manual for a list of supported coders.
SCE	Method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. True = Enabled (On), False = Disabled (Off).

Parameter	Description
RTP Direction	RTP Directional Control. Controlled internally by the device according to the selected coder.
RTCP Direction	RTCP Directional Control. Controlled internally by the device according to the selected coder.
PTime (msec)	Packetization time, i.e., how many coder payloads are combined into a single RTP packet.

The following figure shows the **Media** tab in the Call Details page.

**Figure 8-6: Call Details page - Media tab**



Use the preceding figure as reference to the following explanation of the QoE indicators.

- Local QoE values of MOS, Jitter, Packet loss, Delay and MOS are calculated by the SBC based on RTP packets it receives from the 'remote peer'
- The SBC reports this information to the OVOC using an XML-based, proprietary protocol
- The OVOC displays the information it receives (indicated by 1 in the preceding figure)
- Remote QoE values can be calculated by the 'remote peer' and reported back to the SBC using RTCP packets, except 'Delay' (and RTPC-XR, if supported, for MOS)
- The SBC forwards QoE information (if received) from the 'remote peer' to the OVOC, as described in point 2 above
- The OVOC displays the information it receives (indicated by 2 in the preceding figure) (from 'SBC' to 'remote peer')
- Quality (Good, Fair, Poor), indicated by 3 in the preceding figure, is based on the following criteria:
  - If MOS is received from AudioCodes equipment (SBC) configured with a QOE profile, the 'Quality' displayed matches the profile's thresholds:
    - ◆ Poor = major threshold reached
    - ◆ Fair = minor threshold reached
    - ◆ Good = minor threshold not reached
  - If MOS is received from non-AudioCodes equipment, local settings on the OVOC are used (**System > Configuration > Templates > QoE threshold**)
  - If no MOS information is received, the 'Quality' displayed corresponds to the worst of the 3 QoE values received (Jitter, Packet Loss, Delay)
  - As before, the 'Quality' displayed matches the QoE profile (from the SBC or locally on the OVOC)



MOS gets priority because it's based on algorithms that emulate the human perception of voice quality during a call.

## Signaling

The Signaling tab displays a call's signaling parameters that operators can refer to for diagnostics, troubleshooting and session experience management issues.

**Figure 8-7: Signaling**

CALL DETAILS					
← C: 10.1.1.158:64745 - C: 10.62.0.10:5069 →			← C: 10.10.10.2:5060 - C: 10.9.9.5:5060 →		
MEDIA		SIGNALING		TRENDS	
	+972397...	E-SBC	E-SBC	+972397...	
SIP IP	10.1.1.158		10.62.0.10	10.10.10.2	10.9.9.5
SIP Port	64745		5069	5060	5060
URI	+97239764491@a.com		+972123@adgw01.corp.a.com	39764491@a.com	123@adgw01.corp.com
Output URI Before Map	+97239764491@a.com		+972123@adgw01.corp.com	+97239764491@a.com	+972123@adgw01.corp.a.com
Endpoint Type	SBC		SBC		
SRD	SRDLAN: 1		SRDWAN: 2		
IP Group	Lync ARM: 7		Bezeq SIPT: 3		
SIP IF					
Proxy Set	7		3		
IP Profile	1		3		
Transport Type	TLS		UDP		
Signaling diff server	40		40		

Use the following table as reference to the parameters displayed under the Signaling tab.

**Table 8-6: Signaling Parameters**

Parameter	Description
SIP IP	The call's caller/callee (source/destination) IP address.
SIP Port	The port number used for the SIP call.
URI	The URI (Uniform Resource Identifier) of the caller/callee (source/destination). The SIP URI is the user's SIP phone number (after manipulation, if any). The SIP URI resembles an e-mail address and is written in the following format: sip:x@y:Port, where x=Username and y=host (domain or IP).
Output URI Before Map	The SIP URI address of the caller/callee before manipulation (if any) was done on the URI.
Endpoint Type	Indicates the type of endpoint. For example, 'SBC'.
SRD	The unique name and index configured for the signaling routing domain (SRD). Example: <b>someSRD (n)</b> , where <b>n</b> following the displayed name is the number indicating the SRD's index used to facilitate network configuration.
IP Group	The ID of the IP Group with which the call is associated.
SIP IF	The ID of the SIP Interface with which the call is associated.

Parameter	Description
Proxy Set	The Proxy Set to which the call is associated. This is a group of Proxy servers. Typically, for IP-to-IP call routing, at least two are defined for call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.
IP Profile	The IP Profile assigned to this IP destination call. The IP Profile assigns numerous configuration attributes (e.g., voice codes) per routing rule.
Transport Type	Two options: UDP or TCP
Signaling diff server	The value for Premium Control CoS content (Call Control applications).

## Trends

The Trends tab shows a call's voice quality trend that operators can refer to for diagnostic, troubleshooting and session management experience issues.

**Figure 8-8: Trends**



Voice quality applies to the call's:

- Caller leg
  - caller side (of cloud)
  - device side (of cloud)
- Callee leg
  - callee side (of cloud)
  - device side (of cloud)

### ➤ To assess voice quality:

- Select a quality metric graph option (MOS, Jitter, Packet Loss, Delay and/or Echo) and then select a leg; the graph displayed indicates:
  - the voice quality of the call for the selected quality metric across the selected leg
  - how long the leg lasted
  - the time the leg started and ended



Legs over PSTN are not measured for quality, only legs over IP.

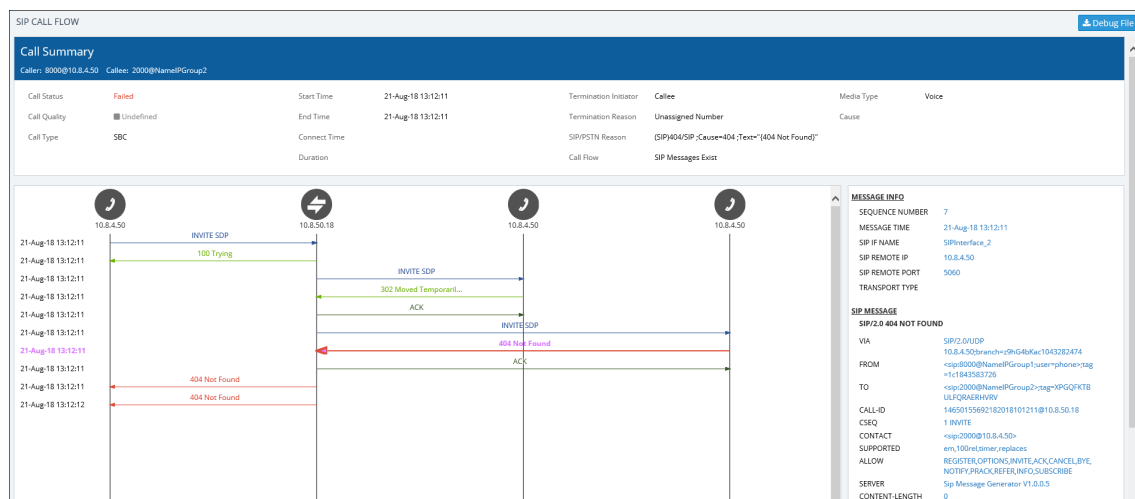
➤ **To compare one voice quality metric with another across different legs:**

1. Select multiple voice quality metric graphs, for example, MOS and Packet Loss, as shown in the figure above.
2. Select a leg option and compare the displayed graphs of quality metrics with one another across this leg.
3. Select another leg and compare the same metrics graphs with one another across this leg.

## SIP Call Flow

The **SIP Call Flow** tab is displayed in the Call Details page when a SIP ladder is available or partially available and found for a specific call over SBC.

**Figure 8-9: SIP Call Flow – Example**



- Click the textual indication of a SIP message to display MESSAGE INFO in the right pane:
  - The text indication changes color to bold pink
  - The call flow leg line is made bold
  - See **404 Not Found** as an example in the figure above



The number of participants indicated in the Call Details and in the Call Flow tabs can be different. The Call Flow tab can include more participants than the Call Details tab, which always includes caller and callee.

The following table shows error response color codes.

The table following it shows SIP message color codes.

**Table 8-7: Error Response Color Codes**

<b>Color</b>	<b>Error Response</b>
Red	Error response message with response code 6xx, 5xx, 4xx, excluding 486 (busy) which is colored green
Green	Error response message with response code 486 (busy) and all other responses
Black	Error response message with response codes 401 and 407

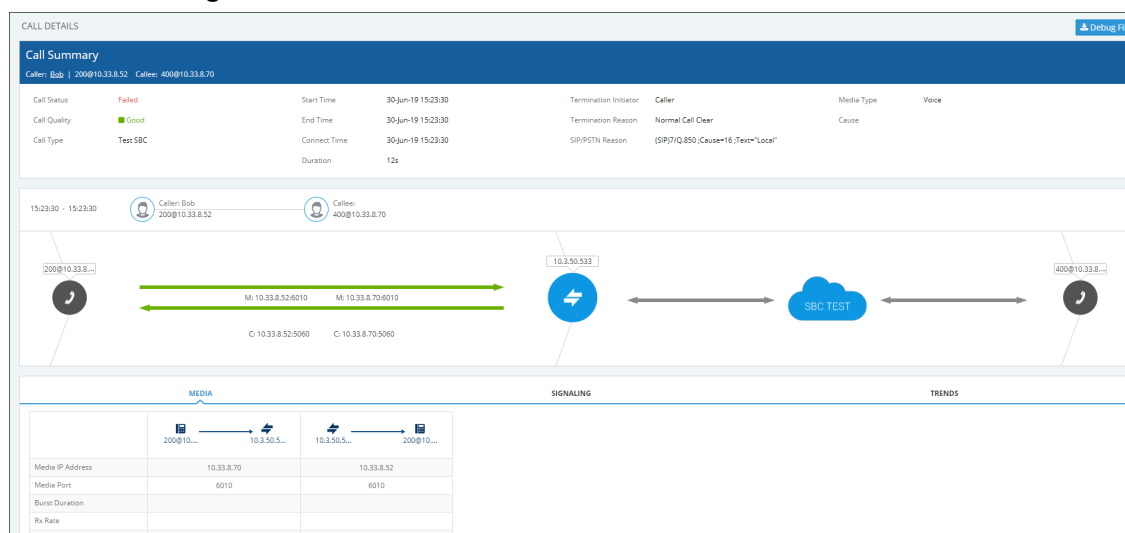
**Table 8-8: SIP Message Color Codes**

<b>Color</b>	<b>SIP Message</b>
Dark Green	ACK
Dark Blue	INVITE
Brown	CANCEL
Purple	BYE
Black (unbolded)	All other SIP messages and codes

## Details of a Test Call Made over an SBC

After filtering calls listed in the Calls List page by clicking **Add Filter > More Filters > Call Type > Test SBC** (see [Filtering by 'More Filters'](#) on page 230), select the test call whose details you want to view and then click the activated **Show** button. The Call Details page that opens displays detailed information about that test call. The following figure shows the details of a test call made over an SBC. The page displays detailed diagnostic information on the call, in textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality.

**Figure 8-10: Call Details – Test Call Over an SBC**



Use the following table as reference to the preceding figure.

**Table 8-9: Call Details - Test Call Made over an SBC**

Page Section	Description
Call Summary (Uppermost)	Indicates the caller's full name and email address and callee's full name and email address.
Call Status	<b>Successful</b> or <b>Failed</b>
Call Quality	<b>Good</b>   <b>Fair</b>   <b>Poor</b> voice quality
Call Type	Test SBC
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the caller began dialing the number to call.
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.
Connect Time	The precise time (hour, minutes and seconds) and date (month, day and year) the connection was established.
Duration	The duration of the call, in seconds.
Termination Initiator	The network entity from which the call was terminated.

Page Section	Description	
Termination Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.	
SIP PSTN Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about the SIP/PSTN Reason.	
Media Type	Voice	
[Quality] Cause	Delay	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
	No value	No value will be displayed for 'Cause' if the quality of the test call is Good. The field will display a value only when call quality is Fair or Poor.
(Middle) Graphic illustration	<ul style="list-style-type: none"> <li>■ Indicates the time the call started and ended</li> <li>■ Visualizes a caller in a call with a callee, including full names and email addresses</li> <li>■ Displays each leg of the call, on both caller and callee side.</li> <li>■ Each leg is: <ul style="list-style-type: none"> <li>✓ Connected to a device</li> <li>✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown)</li> </ul> </li> </ul>	

Page Section	Description
	<ul style="list-style-type: none"> <li>✓ Tagged by C and M C = Control summary (point cursor to view tooltip) M = Media IP address and Port (point cursor to view tooltip)</li> </ul>
(Lowermost) Two tabs	Each opens a page displaying detailed information: <ul style="list-style-type: none"> <li>■ Media (see <a href="#">Media</a> on page 250)</li> <li>■ Signaling (see <a href="#">Signaling</a> on page 236)</li> </ul>

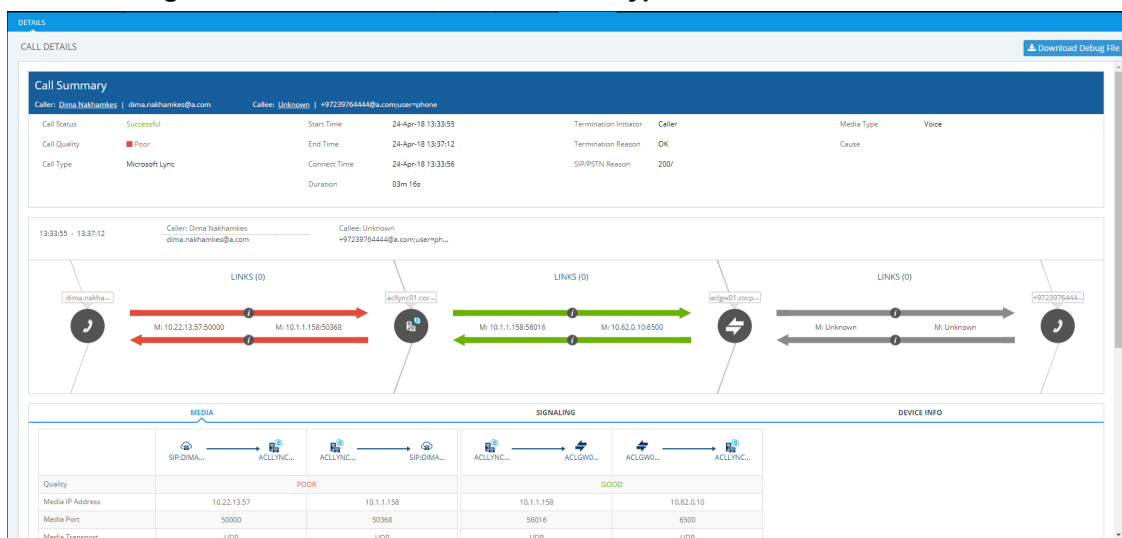
## Call Details Page – Debug File Button

To facilitate troubleshooting if for example there's a discrepancy between the Call Details that the OVOC reports and the call details that you report, you can click a **Debug File** button in the Call Details page to save (download) a debug file in *json* format and then send it to AudioCodes FAEs for analysis.

## Details of a Call Made over Microsoft Skype for Business

The following figure shows the details of a call made over Microsoft Skype for Business. The Details page displays detailed diagnostic information on the call, in textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality.

**Figure 8-11: Call Details - Microsoft Skype for Business**



If there's an issue of poor quality with a call over Microsoft Skype for Business, one of the two legs of the call in the Call Details screen will indicate that there's an issue. The leg that indicates that there's an issue is the leg that scores the worse score of the two legs, i.e., the score indicated in red, as shown in the figure above. Use this table as reference:

**Table 8-10: Call Details - Microsoft Skype for Business**

Page Section	Description
Call Summary (Uppermost)	Indicates the caller's full name and email address and callee's full name and email address.
Call Status	<b>Successful</b> or <b>Failed</b>

Page Section	Description
Call Quality	<b>Good   Fair   Poor</b> voice quality
Call Type	Microsoft Skype for Business
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the caller began dialing the number to call.
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.
Connect Time	The precise time (hour, minutes and seconds) and date (month, day and year) the connection was established.
Duration	The duration of the call, in seconds.
Termination Initiator	The network entity from which the call was terminated.
Termination Reason	<p>The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.</p> <p>Some Skype for Business Termination Reasons are:</p> <ul style="list-style-type: none"> <li>■ OK. Indicates the request was successful.</li> <li>■ Accepted. Indicates that the request has been accepted for processing, but the processing has not been completed.</li> <li>■ No Notification</li> <li>■ Multiple Choices</li> <li>■ Moved Permanently</li> <li>■ Moved Temporarily</li> <li>■ Use Proxy</li> <li>■ Alternative Service</li> </ul>
SIP PSTN Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.
Media Type	Voice

Page Section	Description	
[Quality] Cause	Delay	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
(Middle) Graphic illustration	<ul style="list-style-type: none"> <li>■ Indicates the time the call started and ended</li> <li>■ Visualizes a caller in a call with a callee, including full names and email addresses</li> <li>■ Displays each leg of the call, on both caller and callee side.</li> <li>■ Each leg is: <ul style="list-style-type: none"> <li>✓ Connected to a device</li> <li>✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown)</li> <li>✓ Tagged by C and M <ul style="list-style-type: none"> <li>C = Control summary (point cursor to view tooltip)</li> <li>M = Media IP address and Port (point cursor to view tooltip)</li> </ul> </li> </ul> </li> </ul>	
(Lowermost) Two tabs	Each opens a page displaying detailed information: <ul style="list-style-type: none"> <li>■ Media (see <a href="#">Media</a> on the next page)</li> <li>■ Signaling (see <a href="#">Signaling</a> on page 236)</li> </ul>	

## Media

The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

**Figure 8-12: Media**

DETAILS					
CALL DETAILS					
MEDIA					
SIGNALING					
	SIP-SHAL... → ACLLYNC...		ACLLYNC... → SIP-SHAL...		
	ACLLYNC... → ACLGW0...		ACLGW0... → ACLLYNC...		
Quality	GOOD		GOOD		
Media IP Address	10.11.2.8		10.1.1.158		
Media Port	50008		55924		
Media Transport	UDP		UDP		
Coder	PCMU		PCMU		
MOS	3.71		4.2		
Jitter					
Packet Loss					
Delay	8		7		
Echo					
Signal Level	-10				
Noise Level	-71				
SNR	61				
Burst Duration					
BW Estimation					

Use the following table as reference to the parameters displayed under the Media tab.

**Table 8-11: Media Parameters**

Parameter	Description
Quality	Indicates the call's voice quality: <b>Good</b>   <b>Fair</b>   <b>Poor</b>
Media IP Address	<ul style="list-style-type: none"> <li>The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network.</li> <li>The IP address of the destination host / media network.</li> </ul>
Media Port	<ul style="list-style-type: none"> <li>The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network.</li> <li>Port of the destination host / media network.</li> </ul>
Media Transport	Two options: UDP or TCP
Coder	Up to 10 coders (per group) are supported. See the device manual for a list of supported coders.
MOS	<p>Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises:</p> <p>MOS-LQ = listening quality, i.e., the quality of audio for listening purposes. Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.</p> <p>MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.</p>

Parameter	Description
Jitter	Jitter can result from uneven delays between received voice packets. To space evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
Packet Loss	Lost packets are RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, for the caller and for the callee side. Packet Loss can be more than 100%.
Delay	The round trip delay is the estimated time (in milliseconds) that it takes to transmit a packet between two RTP stations. Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two values are shown, one caller side and another for the callee side.
Echo	The residual echo return loss is the level difference (measured in dB) between the signal transmitted to the listener and the residual echo of that signal.
Signal Level	The ratio of the voice signal level to a 0 dBm0 reference. Signal level = 10 Log10 (RMS talk spurt power (mW)). A value of 127 indicates that this parameter is unavailable.
Noise Level	The ratio of the level of silent-period background noise level to a 0 dBm0 reference. Noise level = 10 Log10 (Power Level (RMS), in mW, during periods of silence). A value of 127 indicates that this parameter is unavailable.
SNR	The ratio of the signal level to the noise level (Signal-Noise Ratio). SNR = Signal level – Noise level.
Burst Duration	The mean duration (in milliseconds), of the burst periods that have occurred since the initial call reception.
BW Estimation	The estimated bandwidth consumed.

## Signaling

The Signaling tab displays a call's signaling parameters that operators can refer to for diagnostics, troubleshooting and session experience management issues.

**Figure 8-13: Signaling**

	MEDIA	SIGNALING
	Caller	Callee
Edge Server		
Gateway		
Mediation Server		
URI	4696@a.com	ami.lahavi@a.com
Phone Number		
Is Internal	true	true
FrontEnd	acilync01.corp.a.com	
Pool	acipool2013.corp.a.com	
Call Priority		Normal

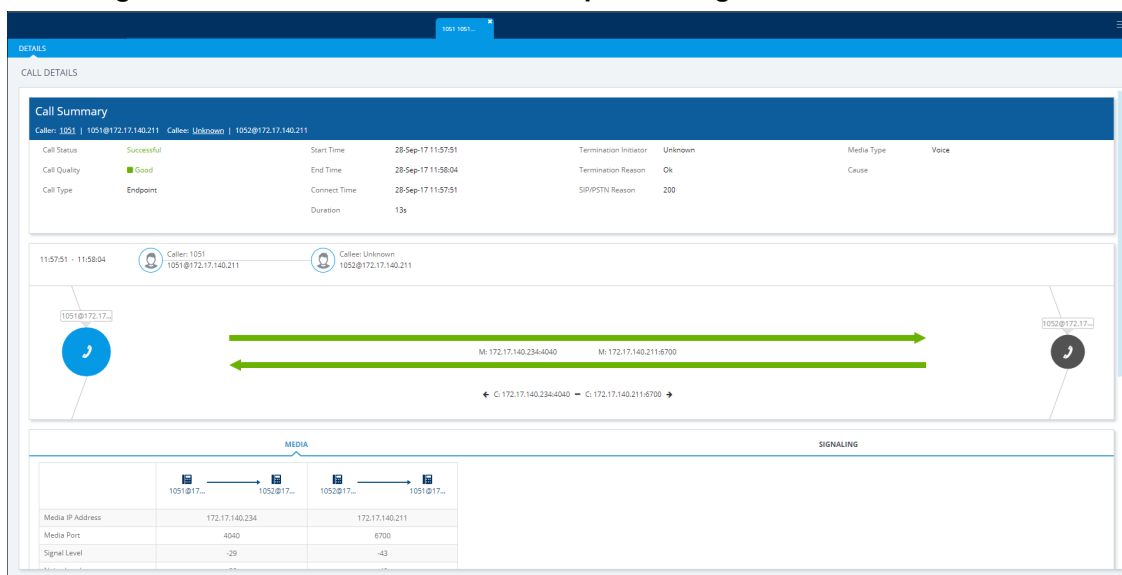
Use the following table as reference to the parameters displayed under the Signaling tab.

**Table 8-12: Signaling Parameters**

Parameter	Description
Edge Server	FQDN of the Edge server used by the user who started (caller) / joined (callee) the session.
Gateway	Gateway of the user who started (caller) / joined (callee) the session.
Mediation Server	Mediation Server of the user who started (caller) / joined (callee) the session.
URI	URI of the user who started (caller) / joined (callee) the session.
Phone Number	Phone URI of the user who started (caller) / joined (callee) the session.
Is Internal	Indicates whether the user who started (caller) / joined (callee) the session logged on from the internal network.
Front End	FQDN of the Front End server that captured the data for the session.
Pool	FQDN of the pool that captured the data for the session.
Call Priority	Call priority of the session.

## Details of a Call Made over an Endpoint Using SIP Publish

The following figure shows the details of a call made over an endpoint using SIP Publish. The Details page displays detailed diagnostic information on the call, in textual format, facilitating effective management, precise diagnosis and targeted remedial action to prevent recurrence of unsuccessful call performance or poor call quality.

**Figure 8-14: Call Details – Over an Endpoint Using SIP Publish**

Use the following table as reference.

**Table 8-13: Call Details - Over an Endpoint Using SIP Publish**

Page Section	Description
Call Summary (Uppermost)	Indicates the caller's full name and email address and callee's full name and email address.
Call Status	<b>Successful</b> or <b>Failed</b>
Call Quality	<b>Good</b>   <b>Fair</b>   <b>Poor</b> voice quality
Call Type	Endpoint
Start Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the caller began dialing the number to call.
End Time	The precise time (hour, minutes and seconds) and date (month, day and year) when the call was terminated.
Connect Time	The precise time (hour, minutes and seconds) and date (month, day and year) the connection was established.
Duration	The duration of the call, in seconds.
Termination Initiator	The network entity from which the call was terminated.
Termination Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about Termination Reason.
SIP PSTN Reason	The reason why the call was terminated. See the device's <i>User's Manual</i> for more information about the SIP/PSTN Reason.
Media Type	Voice

Page Section	Description	
[Quality] Cause	Delay	Delay (or latency) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth. Two Delay values are shown, one value for the caller side and one value for the callee side.
	Echo	The level difference (measured in dB) between the signal transmitted to the listener and the residual echo of this signal.
	Jitter	Jitter can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality. Two Jitter values are shown, one value for the caller side and one value for the callee side.
	MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.
	Packet Loss	Lost packets - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Two Packet Loss % values are shown, one value for the caller side and one value for the callee side. Packet Loss can be more than 100%.
	None	Indeterminate cause
(Middle) Graphic illustration	<ul style="list-style-type: none"> <li>■ Indicates the time the call started and ended</li> <li>■ Visualizes a caller in a call with a callee, including full names and email addresses</li> <li>■ Displays each leg of the call, on both caller and callee side.</li> <li>■ Each leg is: <ul style="list-style-type: none"> <li>✓ Connected to a device</li> <li>✓ Color-coded to indicate voice quality (green = good, yellow = fair, red = poor, grey = unknown)</li> <li>✓ Tagged by C and M <ul style="list-style-type: none"> <li>C = Control summary (point cursor to view tooltip)</li> <li>M = Media IP address and Port (point cursor to view tooltip)</li> </ul> </li> </ul> </li> </ul>	
(Lowermost) Two tabs	Each opens a page displaying detailed information: <ul style="list-style-type: none"> <li>■ Media (see <a href="#">Media</a> on the next page)</li> <li>■ Signaling (see <a href="#">Signaling</a> on page 236)</li> </ul>	

## Media

The Media tab displays a call's media parameter settings that operators can refer to for diagnostics, troubleshooting and session experience management issues.

**Figure 8-15: Media**

DETAILS			
CALL DETAILS			
	MEDIA		SIGNALING
	1051@17...	1052@17...	1051@17...
Media IP Address	172.17.140.234	172.17.140.211	
Media Port	4040	6700	
Signal Level	-29	-43	
Noise Level	-38	-40	
SNR	9	-3	
Rx Rate	62	62	
Quality	GOOD	GOOD	
MOS	4.3	4.3	
Jitter	10	10	
Packet Loss			
Delay	10	8	
Echo			
Coder	G727_32_16		
SCE	false		
RTP Direction	Send Receive		
RTCP Direction	Send Receive		
P-Time	20		

Use the following table as reference.

**Table 8-14: Media Parameters**

Parameter	Description
Media IP Address	<ul style="list-style-type: none"> <li>The IP address of the device source in the operations, administration, maintenance, and provisioning (OAMP) network.</li> <li>The IP address of the destination host / media network.</li> </ul>
Media Port	<ul style="list-style-type: none"> <li>The device's source port in the operations, administration, maintenance, and provisioning (OAMP) network.</li> <li>Port of the destination host / media network.</li> </ul>
Signal Level	The ratio of the voice signal level to a 0 dBm0 reference. Signal level = 10 Log10 (RMS talk spurt power (mW)). A value of 127 indicates that this parameter is unavailable.
Noise Level	The ratio of the level of silent-period background noise level to a 0 dBm0 reference. Noise level = 10 Log10 (Power Level (RMS), in mW, during periods of silence). A value of 127 indicates that this parameter is unavailable.
SNR	The ratio of the signal level to the noise level (Signal-Noise Ratio). SNR = Signal level – Noise level.
Rx Rate	Shows the call's reception rate, in Kbps.
Quality	Voice quality: Good (green), Fair (yellow) OR Red (poor).
MOS	Mean Opinion Score (specified by ITU-T recommendation P.800). Defines the average grade, on a quality scale of Good to Poor, determined after testing calls made over a VoIP network. Comprises:

Parameter	Description
	<p>MOS-LQ = listening quality, i.e., the quality of audio for listening purposes. Doesn't account for bi-directional effects such as delay and echo. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.</p> <p>MOS-CQ = conversational quality; it takes listening quality in both directions into account, as well as the bi-directional effects. Two values are shown: (1) for the device side on the caller leg (2) for the device side on the callee leg.</p>
Jitter	Jitter (in msec) can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality.
Packet Loss	Lost packets, as a percentage - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Packet Loss can be more than 100%.
Delay	Delay (or latency) (in msec) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth.
Echo	The residual echo return loss is the level difference (measured in dB) between the signal transmitted to the listener and the residual echo of that signal.
Coder	Up to 10 coders (per group) are supported. See the device manual for a list of supported coders.
SCE	Method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. True = Enabled (On), False = Disabled (Off).
RTP Direction	RTP Directional Control. Controlled internally by the device according to the selected coder.
RTCP Direction	RTCP Directional Control. Controlled internally by the device according to the selected coder.
PTime (msec)	Packetization time, i.e., how many coder payloads are combined into a single RTP packet.

## Managing QoE Thresholds Profiles per Tenant

The QoE Thresholds page lets you adding a profile of Quality of Experience threshold values, *per tenant*.

For information about adding a *global* (system) QoE Thresholds template, see [QoE Thresholds](#) on page 65.

### ➤ To view QoE thresholds profiles:

- Open the QoE Thresholds page (**Calls > QoE Thresholds**).

**Figure 8-16: QoE Thresholds Profiles**

QOE THRESHOLDS							
DEFAULTS	NAME	DESCRIPTION	MOS	DELAY (MSEC)	PLOSS (%)	JITTER (MSEC)	ECHO (DB)
	Low Sensitivity Threshold		➤3.4➤ ➤1.3➤	➤200➤ ➤1200➤	➤2.7➤ ➤5.5➤	➤45➤ ➤90➤	➤25➤ ➤9➤
⊙ ⊙ ⊙	Medium Sensitivity Threshold		➤3.5➤ ➤2.8➤	➤160➤ ➤500➤	➤2.2➤ ➤5➤	➤40➤ ➤80➤	➤20➤ ➤10➤
	High Sensitivity Threshold		➤3.6➤ ➤2.9➤	➤140➤ ➤400➤	➤1.5➤ ➤4.3➤	➤35➤ ➤70➤	➤27➤ ➤11➤
	Low Sensitivity Threshold		➤3.4➤ ➤2.7➤	➤200➤ ➤1200➤	➤2.7➤ ➤5.5➤	➤45➤ ➤90➤	➤25➤ ➤9➤
⊙ ⊙ ⊙	Medium Sensitivity Threshold		➤3.5➤ ➤2.8➤	➤160➤ ➤500➤	➤2➤ ➤5➤	➤40➤ ➤80➤	➤20➤ ➤10➤
	High Sensitivity Threshold		➤3.6➤ ➤2.9➤	➤140➤ ➤400➤	➤1.5➤ ➤4.3➤	➤35➤ ➤70➤	➤27➤ ➤11➤
	Low Sensitivity Threshold		➤3.4➤ ➤2.7➤	➤200➤ ➤1200➤	➤2.7➤ ➤5.5➤	➤45➤ ➤90➤	➤25➤ ➤9➤
⊙ ⊙ ⊙	Medium Sensitivity Threshold		➤3.5➤ ➤2.8➤	➤160➤ ➤500➤	➤2➤ ➤5➤	➤40➤ ➤80➤	➤20➤ ➤10➤
	High Sensitivity Threshold		➤3.6➤ ➤2.9➤	➤140➤ ➤400➤	➤1.5➤ ➤4.3➤	➤35➤ ➤70➤	➤27➤ ➤11➤

In the page you can:

- view QoE thresholds profiles and their metrics thresholds
- add a profile (see [Adding a QoE Thresholds Profile per Tenant](#) on page 254)
- edit or delete an existing profile (see [Editing a QoE Thresholds Profile per Tenant](#) on page 257 and [Deleting a QoE Thresholds Profile per Tenant](#) on page 257)

## Understanding the 3 Sensitivity-Level Profiles

The following table shows the monitored parameters MOS, Delay, Packet Loss and Jitter, each associated with each of the 3 sensitivity-level profiles: Low, Default and High. Each parameter's Green-Yellow Threshold and Yellow-Red Threshold differ in association with the configured Profile.

For each monitored parameter, administrators can use the thresholds in the predefined profile, or define their own thresholds.

**Table 8-15: Quality Profile Parameters**

Parameter (units)	Sensitivity Level	Good-Fair (Green-Yellow) Threshold	Fair-Poor (Yellow-Red) Threshold
MOS	Low	3.4	2.7
	Medium	3.5	2.8
	High	3.6	2.9
Delay (msec)	Low	200	1200
	Medium	160	500
	High	140	400

Parameter (units)	Sensitivity Level	Good-Fair (Green-Yellow) Threshold	Fair-Poor (Yellow-Red) Threshold
Packet Loss (%)	Low	2.7	6.6
	Medium	2	5
	High	1.5	4.3
Jitter (msec)	Low	45	90
	Medium	40	80
	High	35	70
Echo (dB)	Low	23	9
	Medium	25	10
	High	27	11

## Understanding How Call Color is Determined

It may be useful for you to understand how Skype for Business call color is determined. As shown previously, a default profile is assigned to each Front End server, which you can change. (No profile is attached to the Mediation Server or Edge Server).

A default profile is also assigned to each Link, which you can change and apply to each Link as shown previously.

### Link Profile as Determinant

Each call comprises one or more legs. Each leg is assigned a color, determined by its associated Link profile. If a call leg passes over few Links and each has a different profile, each Link has its own color (displayed in the Summary Panes) corresponding to its profile. However, the call leg's color is set as the worst color received from all the Links profile; the Call Details screen shows what profile caused the leg color. If a call leg does not match any of the Links, its color is defined based on the FE profile. The color representing worst quality among all the legs will be the call color. (If a call comprises only from one leg, the color of the leg will be the call color).

### MOS Metric as Determinant

Each profile can be configured with a set of quality metrics (MOS / Packet Loss / Jitter / Delay / Echo). Each call leg's color is determined at the end of the call using its reported metrics. If MOS is reported, the leg will be determined by the MOS' color; if not, the color representing worst quality will be the leg's color. If any of the call leg's reported metrics are excluded from the profile, color calculations will ignore this metric.

## Adding a QoE Thresholds Profile per Tenant

You can add a QoE Thresholds profile.

➤ **To add a QoE thresholds profile:**

1. Open the QoE Thresholds page (**Calls > QoE Thresholds**).
2. Click **Add**.

**Figure 8-17: QoE Thresholds Details**

**QOE THRESHOLDS DETAILS**

Threshold Name \*

Description

Tenant \*

Attachments: 0 Devices, 0 Links, 0 Sites, 0 Endpoints [View](#)

Defaults: All | None | Invert  
☐ Device ☐ Link ☐ Endpoint

---

THRESHOLD VALUES

**Status Threshold Values**

<input checked="" type="checkbox"/> MOS (0-5)	<input type="text" value="2.5"/>	<input type="text" value="3.5"/>
<input checked="" type="checkbox"/> Delay (Msec)	<input type="text" value="500"/>	<input type="text" value="160"/>
<input checked="" type="checkbox"/> PLoss (%)	<input type="text" value="5"/>	<input type="text" value="2"/>
<input checked="" type="checkbox"/> Jitter (Msec)	<input type="text" value="80"/>	<input type="text" value="40"/>
<input checked="" type="checkbox"/> Echo (DB)	<input type="text" value="10"/>	<input type="text" value="25"/>

**OK** **Close**

3. Provide an intuitive name for the profile. Use the names of the three predefined QoE profiles, displayed in the QoE Threshold Details screen following, as a reference.
4. In the 'Description' pane, provide an intuitive, friendly description to facilitate future operator management.
5. From the 'Tenant' drop-down, select the tenant for whom you're customizing this profile.
6. Next to 'Attachments', click the **View** button.

Figure 8-18: Attachments

**QOE THRESHOLDS DETAILS**

Threshold Name \*

Description

Tenant \* ErezTenant

Attachments: 0 Devices, 0 Links, 0 Sites, 0 Endpoints [View](#)

Defaults:

Search by name

- ErezTenant
  - ErezRegion-1
    - ErezRegion-2
      - devices
        - links
          - utgfytf

☒ MOS (0-5)

☒ Delay (Msec)

☒ PLoss (%)

☒ Jitter (Msec) → 80 → 40 →

☒ Echo (DB) → 10 → 25 →

OK Close

- Expand the tenant to navigate to and select the entities to which to attach this QoE thresholds profile (devices, links or endpoints).
- Next to 'Defaults', select:
  - Devices** in order to set this QoE thresholds profile as the default for all devices. If selected, then every new device that is added to the tenant is automatically set with this QoE thresholds profile and all *previous* devices' default QoE thresholds profile is set with this new default profile.
  - Links** in order to set this QoE thresholds profile as the default for all links. If selected, then every new link that is added to the tenant is automatically set with this QoE thresholds profile and all *previous* links' default QoE thresholds profile is set with this new default profile.
  - Endpoints** in order to set this QoE thresholds profile as the default for all endpoints. If selected, then every new endpoint that is added to the tenant is automatically set with this QoE thresholds profile and all *previous* endpoints' default QoE thresholds profile is set with this new default profile.
- Specify which voice quality metrics to include in or exclude from the profile. You can exclude, for example, the metrics of 'MOS', 'Delay' and 'Echo', but include 'Packet Loss' and 'Jitter'. To *exclude* a voice quality metric, clear its check box. By default, all voice quality metrics are included in the profile.

10. Enter the MOS metric's thresholds (for example). Enter the other metrics' thresholds. The following figure shows the profile 'Medium Sensitivity Threshold' as an example.

**Figure 8-19: QoE Thresholds Settings - Medium Sensitivity Threshold**

The screenshot shows a dialog box titled "QOE THRESHOLDS DETAILS" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Threshold Name \***: Medium Sensitivity Threshold
- Description**: (Empty text area)
- Tenant**: Tenant2
- Attachments**: 0 Devices, 0 Links, 0 Sites, 0 Endpoints [View](#)
- Defaults**: All | None | Invert
  - ☒ Device ☒ Link ☒ Endpoint
- THRESHOLD VALUES** (Section Header)
- Status Threshold Values** (Section Header)
- MOS (0-5)**: ☒ [Green arrow] 3 [Yellow arrow] [Yellow arrow] 3.5 [Red arrow]
- Delay (Msec)**: ☒ [Green arrow] 500 [Yellow arrow] [Yellow arrow] 160 [Red arrow]
- PLoss (%)**: ☒ [Green arrow] 5 [Yellow arrow] [Yellow arrow] 2 [Red arrow]
- Jitter (Msec)**: ☒ [Green arrow] 80 [Yellow arrow] [Yellow arrow] 40 [Red arrow]
- Echo (DB)**: ☒ [Green arrow] 10 [Yellow arrow] [Yellow arrow] 25 [Red arrow]

At the bottom of the dialog are two buttons: **OK** and **Close**.

11. Click **OK**; the profile is displayed in the QoE Thresholds page.
12. In the page, select the profile; the QoE Threshold Details are displayed.

Figure 8-20: QoE Threshold Details

QOE THRESHOLDS									
<a href="#">Add</a> <a href="#">Edit</a> <a href="#">Delete</a> <a href="#">Refresh</a>									
DEFAULTS	NAME	TENANT	DESCRIPTION	MOS	DELAY (MSEC)	PLOSS (%)	JITTER (MSEC)	ECHO (DB)	
	Low Sensitivity Threshold	Tenant1		+3.4 +2.9	+200 +1,200	+2.7 +6.6	+45 +90	+25 +9	
	Medium Sensitivity Threshold	Tenant1		+3.5 +3	+160 +500	+2 +5	+40 +80	+25 +10	
	High Sensitivity Threshold	Tenant1		+3.6 +3.1	+140 +400	+1.5 +4.3	+35 +70	+27 +11	
	Hf bjh uyhyuyhyuyhyuyh...	Tenant1		+3.5 +2.5	+160 +500	+2 +5	+40 +80	+25 +10	
	4lk	Tenant1		+3.5 +2.5	+160 +500	+2 +5	+40 +80	+25 +10	
	Low Sensitivity Threshold	Tenant2		+3.4 +2.9	+200 +1,200	+2.7 +6.6	+45 +90	+25 +9	
	Medium Sensitivity Threshold	Tenant2		+3.5 +3	+160 +500	+2 +5	+40 +80	+25 +10	
	High Sensitivity Threshold	Tenant2		+3.6 +3.1	+140 +400	+1.5 +4.3	+35 +70	+27 +11	
	Hf bjh uyhyuyhyuyhyuyh...	Tenant2		+3.5 +2.5	+160 +500	+2 +5	+40 +80	+25 +10	
	4lk	Tenant2		+3.5 +2.5	+160 +500	+2 +5	+40 +80	+25 +10	
	Low Sensitivity Threshold	h		+3.4 +2.9	+200 +1,200	+2.7 +6.6	+45 +90	+25 +9	
	Medium Sensitivity Threshold	h		+3.5 +3	+160 +500	+2 +5	+40 +80	+25 +10	
	High Sensitivity Threshold	h		+3.6 +3.1	+140 +400	+1.5 +4.3	+35 +70	+27 +11	
	Hf bjh uyhyuyhyuyhyuyh...	h		+3.5 +2.5	+160 +500	+2 +5	+40 +80	+25 +10	
	4lk	h		+3.5 +2.5	+160 +500	+2 +5	+40 +80	+25 +10	
	Low Sensitivity Threshold	r		+3.4 +2.9	+200 +1,200	+2.7 +6.6	+45 +90	+25 +9	
	Medium Sensitivity Threshold	r		+3.5 +3	+160 +500	+2 +5	+40 +80	+25 +10	
	High Sensitivity Threshold	r		+3.6 +3.1	+140 +400	+1.5 +4.3	+35 +70	+27 +11	
	Hf bjh uyhyuyhyuyhyuyh...	r		+3.5 +2.5	+160 +500	+2 +5	+40 +80	+25 +10	

QOE THRESHOLD DETAILS

NAME: Medium Sensitivity Threshold

TENANT: Tenant2

DESCRIPTION:

MOS: +3.5 +3

DELAY (MSEC): +160 +500

PLOSS (%): +2 +5

JITTER (MSEC): +40 +80

ECHO (DB): +25 +10

Attached Items

DEVICES: 0

LINKS: 0

ENDPOINTS: 0

DEFAULT DEVICES: 0

DEFAULT LINKS: 0

DEFAULT ENDPOINTS: 0

The QoE Threshold Details window displays under **Attached Items** the number of devices / links / endpoints to which the selected profile is attached.

In the QoE Threshold Details window:

➔ **x** ➔ indicates the *lower* threshold of the quality metric:

- Up until the threshold value of **x** is reached = **green** = good voice quality
- If the threshold value of **x** is exceeded = **yellow** = fair voice quality

➔ **y** ➔ indicates the *upper* threshold of the quality metric:

- Up until the threshold value of **y** is reached = **yellow** = fair voice quality
- If the threshold value of **y** is exceeded = **red** = poor voice quality

## Editing a QoE Thresholds Profile per Tenant

You can edit an existing QoE Thresholds profile per Tenant.

### ➤ To edit a QoE Thresholds profile:

- In the QoE Thresholds page (**Calls > QoE Thresholds**), select the profile to edit and click **Edit**; the screen shown under [Adding a QoE Thresholds Profile per Tenant](#) on page 254 opens. Refer to the instructions under the figure.

## Deleting a QoE Thresholds Profile per Tenant

You can delete a QoE Thresholds profile per Tenant.

### ➤ To delete a QoE Thresholds profile per Tenant:

- In the QoE Thresholds page (**Calls > QoE Thresholds**), select the profile to delete and click **Delete**. Note that default profiles cannot be deleted.

## Managing QoE Status and Alarms per Tenant

The QoE Status & Alarms page lets you manage QoE statuses and alarms *per tenant*.

For information about managing *global (system-wide)* QoE statuses and alarms, see [QoE Status and Alarms](#) on page 67.

➤ **To view QoE statuses and alarms per tenant:**

- From under the Calls menu, open the QoE Status & Alarms page (**Calls > QoE Status & Alarms**).

**Figure 8-21: QoE Status & Alarms**

QOE STATUS & ALARMS <span>⊕ Add</span> <span>✎ Edit</span> <span>🗑 Delete</span>										
DEFAULTS	NAME	LAST RUNTIME	MONITORING F...	MINIMUM CALL...	FAILED CALLS PROFILE...	POOR QUALITY CALLS...	AVERAGE CALL DURATL...	BANDWIDTH RULE (KB/...	MAX CONCURRENT CA...	DESCRIPTION
⊕ ⊖ ⊕ ...	ALARM RULE	31-Jul-17 14:58:...	15	50	+5+ +10+ 🚫	+5+ +10+ 🚫	+5+ +3+ 🚫	+0+ +1+ 🚫	+0+ +1+ 🚫	
⊕ ⊖ ⊕ ...	ALARM RULE	31-Jul-17 14:58:...	15	50	+2+ +10+ 🚫	+2+ +10+ 🚫	+5+ +3+ 🚫	+0+ +1+ 🚫	+0+ +1+ 🚫	
⊕	S4B failed calls	31-Jul-17 14:58:...	15	10	+5+ +10+ 🚫	+5+ +10+ 🚫	+5+ +3+ 🚫	+5+ +10+ 🚫	+5+ +10+ 🚫	
⊕ ⊖ ⊕ ...	ALARM RULE	31-Jul-17 14:58:...	15	50	+2+ +10+ 🚫	+2+ +10+ 🚫	+5+ +3+ 🚫	+0+ +1+ 🚫	+0+ +1+ 🚫	

The information displayed in the page above - QoE Status & Alarms *per tenant* – is identical to the information displayed in the *global (system-wide)* QoE Status & Alarms page. See [QoE Status and Alarms](#) on page 67 for a detailed description.

## Adding a QoE Alarm Rule per Tenant

You can add a new rule for a QoE alarm per tenant.

➤ **To add a new QoE alarm rule per tenant:**

1. From the QoE Status & Alarms page, open the QoE Status & Alarms Settings screen (**Calls > QoE Status & Alarms** and then click **Add**).

**Figure 8-22: QoE Status & Alarms Settings**

**QOE STATUS & ALARMS DETAILS**

Name \*

Description

Tenant \*

Attachments: 0 Devices, 0 Links, 0 Sites, 0 Endpoints [View](#)

Defaults: All | None | Invert  
☐ Device ☐ Link ☐ Site ☐ Endpoint

Monitoring Frequency Min

Minimum Call Per Entity To Analyze

---

THRESHOLD VALUES

	Status Threshold Values		Generate Alarm
Failed Calls Alarm (Calls %):	<input type="text" value="2"/>	<input type="text" value="10"/>	<input checked="" type="checkbox"/>
Poor Quality Calls Alarm (Calls %):	<input type="text" value="2"/>	<input type="text" value="10"/>	<input checked="" type="checkbox"/>
Avg Call Duration Alarm (sec):	<input type="text" value="5"/>	<input type="text" value="3"/>	<input checked="" type="checkbox"/>
Bandwidth Alarm (Kb/sec):	<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="checkbox"/>
Max Concurrent Calls Alarm (Calls #):	<input type="text" value="5"/>	<input type="text" value="10"/>	<input type="checkbox"/>

2. Configure the parameters using the following table as reference.

**Table 8-16: QoE Status & Alarms Settings**

Parameter	Description
Name	Enter an operator-friendly alarm rule name to facilitate intuitive effective management later.
Description	Describe the alarm rule to facilitate effective management later.
Attachments	Click <b>View</b> and then navigate to and select the entities to which to attach this QoE Alarm Rule: devices, links, sites and/or endpoints.
Defaults	Select the <b>Device</b> , <b>Link</b> , <b>Site</b> and/or <b>Endpoint</b> monitoring filter. <ul style="list-style-type: none"> <li>If you select <b>Link</b>, the links selection pop-up opens; select the links to monitor (the default is <b>All Selected</b>).</li> <li>If you select <b>Device</b>, the device selection pop-up opens; select the devices to monitor (the default is <b>All Selected</b>).</li> </ul>

Parameter	Description
Monitoring Frequency (min)	Determines how frequently the OVOC automatically performs data analysis. Defines every 15 (default), 30 or 60 minutes.
Minimum Calls to Analyze	Defines the number of calls to analyze. Default = 50 calls. Up to 1000 calls can be defined. If the number of calls made doesn't exceed the defined # of calls to analyze, the OVOC won't perform data analysis.
Failed Calls Alarm	Select the <b>Generate Alarm</b> option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: <b>5%</b> of calls (default); if this threshold is exceeded, the alarm is triggered. Major Threshold: <b>3%</b> of calls (default); if this threshold is exceeded, the alarm is triggered.
Poor Quality Calls Alarm	Select the <b>Poor Quality Calls Alarm</b> option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: <b>10%</b> of calls (default); if this threshold is exceeded, the alarm is triggered. Major Threshold: <b>8%</b> of calls (default); if this threshold is exceeded, the alarm is triggered.
Avg Call Duration Alarm	Select the <b>Avg Call Duration Alarm</b> option to active the alarm. Clear the option to deactivate the alarm. Critical Threshold: <b>5</b> seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered. Major Threshold: <b>10</b> seconds (default), up to 100 seconds; if the average duration of calls is below this, the alarm is triggered.
Bandwidth Alarm	Select the <b>Bandwidth Alarm</b> option to active the alarm. Clear the option to deactivate the alarm. Major Threshold: if the bandwidth falls below or exceeds the value you configure (minimum of <b>0</b> Kbps and a maximum of <b>1000000</b> Kbps), an alarm of Major severity is triggered. Critical Threshold: if the bandwidth falls below or exceeds the value you configure (minimum of <b>0</b> Kbps and a maximum of <b>1000000</b> Kbps), an alarm of Critical severity is triggered. <ul style="list-style-type: none"> <li>■ You must configure a <i>higher</i> value for the <i>Critical</i> Threshold than for the Major Threshold.</li> <li>■ You can configure a minimum of <b>0</b> Kbps and a maximum of <b>1000000</b> Kbps for either the Critical or the Major Threshold, so long as the value you configure for the <i>Critical</i> Threshold is higher than the value you configure for the Major Threshold.</li> </ul>
Max Concurrent Calls Alarm	Select the <b>Max Concurrent Calls Alarm</b> option to active the alarm. Clear the option to deactivate the alarm. Major Threshold: if the the number of concurrent calls falls below, or exceeds, the value you configure (minimum of <b>0</b> and a maximum of <b>100000</b> ), an alarm of Major severity is triggered. Critical Threshold: if the number of concurrent calls falls below, or exceeds, the value you configure (minimum of <b>0</b> and a maximum of <b>100000</b> ), an alarm of Critical severity is triggered.

Parameter	Description
	<ul style="list-style-type: none"> <li>You must configure a <i>higher</i> value for the <i>Critical</i> Threshold than for the Major Threshold.</li> <li>You can configure a minimum of <b>0</b> and a maximum of <b>1000000</b> for either the Critical or the Major Threshold, so long as the value you configure for the <i>Critical</i> Threshold is higher than the value you configure for the Major Threshold.</li> </ul>

- Click **OK**; the QoE alarm rule is now listed in the QoE Status & Alarms page.

## Editing a QoE Alarm Rule per Tenant

You can edit a QoE alarm rule per tenant.

### ➤ To edit a QoE alarm rule per tenant:

- In the QoE Status & Alarms page (**Calls > QoE Status & Alarms**), select the QoE alarm rule to edit and then click **Edit**; the Alarm Rule Details screen opens displaying parameters identical to those displayed when adding a rule. Use the table above as reference.

## Deleting a QoE Alarm Rule

You can delete a QoE alarm rule if necessary.

### ➤ To delete a QoE alarm rule:

- In the QoE Status & Alarms page (**Calls > QoE Status & Alarms**), select the QoE alarm rule to delete and then click **Delete**. Note that default QoE alarm rules cannot be deleted.

## 9 Getting Information on Users Experience

The OVOC enables you to get information on how end users experience IP network telephony.



'End users' refers to an enterprise's employees. By contrast, 'operators' refers to administrators managing the enterprise's network using the OVOC.

Adding an Active Directory to the OVOC below shows how to add an Active Directory in the Active Directories page.

[Assessing Overall End Users Experience](#) on page 266 and [Assessing a Specific End User's Experience](#) on page 268 show how to get user experience info in the Users Experience page.

[Adding an Active Directory to the OVOC](#) below shows how to manage end users in the User Details page.

**Figure 9-1: Getting Information on Users**

USERS EXPERIENCE

Show

Refresh

USERS FILTERS

ADD FILTER

REAL TIME

FULL NAME	USER NAME	CALLS COUNT	TOTAL DURATION	SUCCESS / FAILED	CALL QUALITY	MOS	JITTER	DELAY	PACKET LOSS	DESCRIPTION
Israel Zismanovich	israelz	4	19m 01s	<div></div>	4.3	1.5	18.3	0		Compliance Manager
Kevin Fleming	kevinf	5	34m 32s	<div></div>	4.3	2.3	23.7	0		Sales Engineer
Moshe Mizrahi	moshe	8	04m 13s	<div></div>	4.3	7.8		0		Director of IT
Amir Hagan	amirha	10	25m 45s	<div></div>	4.1	1	28.3	0		Network and Security Tea...
Shir Soffer	shirso	2	04m 20s	<div></div>	4.3	1	22.3	0		System Administrator
Yuval Yotse	yuvay	5	22m 26s	<div></div>	4.3	0.5	40.5	0		DevOps Engineer
Lavi Elias	lavie	1	03m 12s	<div></div>	4	9	40	0		AI/ML Team Leader
Yehiel Zohar	yehielz	5	01m 44m 32s	<div></div>	4.3	2	7.7	0		SW Engineer
Shuly Reichert	shulyr	14	03m 38m 50s	<div></div>	4.2	1.2	29.2	0		DevOps Team Leader
Rudion Koren	rudiank	6	38m 15s	<div></div>	4.2	1.2	18.8	0		Vocalcom QA Eng
El Drouel	elish	1	29s	<div></div>	4.3	1	17	0		DSP Group Manager
Ran Greenberg	ranng	5	22m 13s	<div></div>	3.9	2.2	5.3	0		SW Engineer
Glad Moyal	gladm	12	25m 48s	<div></div>	4.1	1.2	27	0		Customer Support & Inte...
Roni Pessach	ronip	17	16m 02s	<div></div>	3.9	2.2	6.8	0		CAS Leader
Zeev Bodnev	zeevb	1	03m 21s	<div></div>	4.1	2	22	0		Testing Engineer
Hadas Aizal	hadasa	3	02m 30s	<div></div>	4.3	0.7	15.3	0		SW Engineer
Aviv Shmueli	avivsh	9	08m 42s	<div></div>	4.1	1.1	11	0		CP Team Leader
Derisim Even Tzur	derisim	15	02m 03m 54s	<div></div>	4.1	1.6	8.7	0		QA Team Leader
Benny Yossifson	bennyy	2	14m 04s	<div></div>	3.9	2.5	6	0		RMA Team Leader
Yael Hemo	yaelh	5	03m 49s	<div></div>	4.3	51.5	13.3	2.7		QA Engineer

## Adding an Active Directory to the OVOC

You can add an Active Directory to the OVOC.

➤ **To add an Active Directory to the OVOC:**

1. Open the Active Directory page (**Users > Active Directories**).

### Figure 9-2: Active Directories

USERS EXPERIENCE

USER DETAILS

ACTIVE DIRECTORIES

ACTIVE DIRECTORIES

Add

Edit

Sync Now

Delete

Refresh

✓

ACL-AD

3344 users

!

activeDirectories\_test

0 users

2. Click **Add**.

**Figure 9-3: Active Directory Settings**

ACTIVE DIRECTORY DETAILS

**GENERAL**      **SYNCHRONIZATION**

Name \*

Tenant \* Zipora2

Host \*

Port \* 389

Base object \*

Bind DN \*

Password \*

Enable SSL ☐

Certificate File

Verify Certificate Subject Name ☐

Test Connectivity

OK Close

3. Configure the General AD settings using the following table as reference.

**Table 9-1: Active Directory Settings - General**

Setting	Description
Name	Enter an intuitive name for the AD to facilitate operator management later.
Tenant	From the drop-down, select the tenant configured as shown in <a href="#">Adding a Tenant</a> on page 85.
Host	Consult with the IT manager responsible for the AD in your enterprise.
Port	The default is typically 389 but consult with the IT manager responsible for the Active Directory in your enterprise.
Base object	Enterprise employees are listed under branches/departments in a tree structure. Enter in the field the branch/department whose employees the AD manages. The AD will then access only to that (relevant) branch/department's employees. For more information, consult with the IT manager responsible for the Active Directory in your enterprise.
Bind DN	For the 'DN' (Domain Name) field, consult with the IT manager responsible for the Active Directory in your enterprise.

Setting	Description
Password	Consult with the IT manager responsible for the AD in your enterprise.
Enable SSL	Select the option to secure the connection with the AD server over SSL; an HTTPS connection between the OVOC and the LDAP server is opened. Clear (default) the option for the connection with the LDAP server to be non-secured.
Certificate file	This option is only activated if the 'Enable SSL' option described before was selected. From the drop-down, select the certificate file that you want to use to secure the SSL connection with the LDAP server. The OVOC authenticates the SSL connection using the certificate. Make sure you load the SSL certificate file, required by the LDAP Active Directory platform, to the Software Manager, as described in <a href="#">Adding Configuration Files to the OVOC's Software Manager</a> on page 72.
Test connectivity (NA)	Click to test synchronization of the OVOC and the Active Directory databases. You can alternatively click <b>Sync Now</b> in the Active Directories page.
Verify Certificate Subject Name	This option is only activated if the 'Enable SSL' option described previously was selected and a 'Certificate file' was selected from the drop-down list.  Select this option to enable authentication of the hostname (FQDN) sent in the Certificate file by the LDAP server. The option provides an additional means of securing the SSL connection between the OVOC server and the LDAP server.

4. Click the **Synchronization** tab.

The screenshot shows a window titled 'ACTIVE DIRECTORY DETAILS' with a close button (X) in the top right corner. It has two tabs: 'GENERAL' and 'SYNCHRONIZATION'. The 'SYNCHRONIZATION' tab is selected. Under this tab, there are three input fields: 'Check for updates every (hours)' with a value of 1, 'Perform full update every (days)' with a value of 3, and 'At' with a time set to 0:00.

5. Configure the AD settings - Synchronization tab settings using the following table as reference.

**Table 9-2: Active Directory Settings - Synchronization**

Setting	Description
Check for updates every....hours	Lets you schedule how frequently synchronization of the OVOC and the Active Directory databases takes place. After synchronization is performed, the OVOC's User Details page is updated to reflect the Active Directory.
Perform full update every....days	Lets you schedule how frequently a full synchronization is performed. Select from a range of 1-7, i.e., once a day (most frequent) to once a week (most infrequent). After synchronization is performed, the OVOC's User Details page is updated to reflect the Active Directory.

Setting	Description
At 0:0	Lets you schedule the time at which the full synchronization is performed. After it's performed, the OVOC's User Details page is updated to reflect the Active Directory.

- Click **OK**.

## Editing an Active Directory

You can edit an Active Directory after adding one.

### ➤ To edit an Active Directory:

- Open the Active Directory page (**Users > Active Directories**).
- Select the Active Directory to edit and click now-enabled **Edit** button.

**Figure 9-4: Active Directory Settings**

**ACTIVE DIRECTORY SETTINGS** [X]

**GENERAL**

Tenant:

Name:  Host:  Port:

Base object:

Bind DN:

Password:

☐ Enable SSL Certificate file:  [v]

**UPDATES**

Check for updates every  hours

Perform full update every  days

at  :

- Edit the parameters using the table [Adding an Active Directory to the OVOC](#) on page 262 as reference, and then click **OK**.

## Deleting an Active Directory

You can delete an Active Directory if necessary.

### ➤ To delete an Active Directory:

1. Open the Active Directory page (**Users > Active Directories**).
2. Select the Active Directory to delete and click now-enabled **Delete** button.

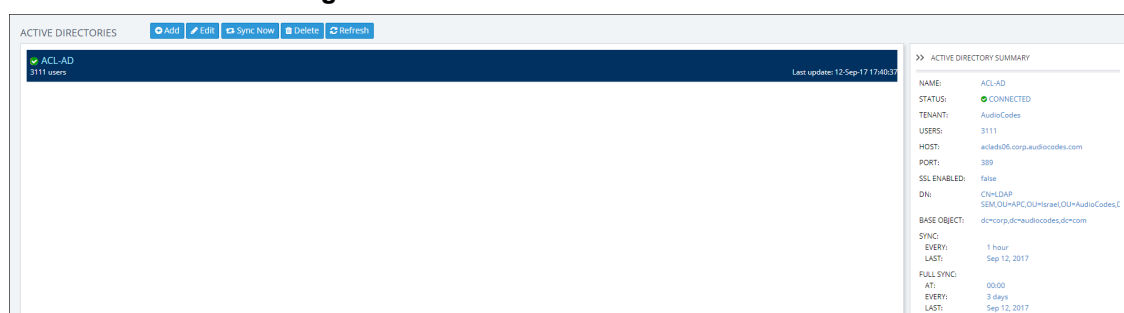
## Synchronizing an AD with the AD Server

You can manually synchronize an AD with the AD server.

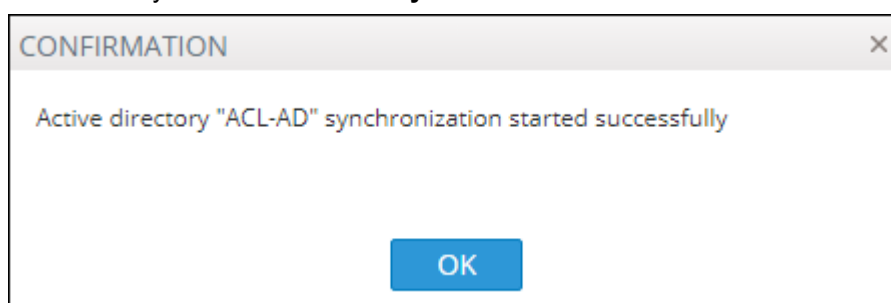
### ➤ To synchronize an AD with the AD server:

1. Open the Active Directories page (**Users > Active Directories**).

**Figure 9-5: Active Directories**



2. Select the AD to synchronize and click **Sync Now**.



3. In the confirmation prompt, click **OK**.

## Assessing Overall End Users Experience

The OVOC enables operators to assess at a glance the overall experience of end users and to tweak the enterprise's telephony network to enhance their experience. Users experience includes statistics related to voice quality (good, fair and poor quality voice) and statistics related to call performance (rate and number of successful versus failed calls).

### ➤ To assess end users experience:

1. Open the Users Experience page (**Users > Users Experience**).

**Figure 9-6: Users Experience**

USERS EXPERIENCE

Show

Refresh

USER FILTERS

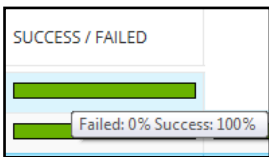
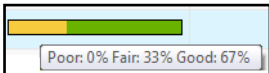
ADD FILTER

REAL TIME

Full Name	User Name	Calls Count	Total Duration	Success / Failed	Call Quality	MOS	Jitter	Delay	Packet Loss	Description
Israel Zismanovich	israelz	7	12m 34s	<div><div></div></div>	<div><div></div></div>	3.9	3	6	0	Compliance Manager
Remco Westerman	remcow	3	15m 56s	<div><div></div></div>	<div><div></div></div>	4.2	3	201	0	Senior Support Engin...
Walter Van Schaik	WalterV	2	04m 03s	<div><div></div></div>	<div><div></div></div>	4.2	0.5	74.5	0	Chief Architect
Moshe Mizrahi	moshe	2	01m 20s	<div><div></div></div>	<div><div></div></div>	4.4	3	31	0	Director of IT
Amir Kagan	amirka	10	54m 25s	<div><div></div></div>	<div><div></div></div>	4.2	3.2	27.2	2.8	Network and security...
Shai Sefer	shatso	3	06m 57s	<div><div></div></div>	<div><div></div></div>	4.3	1.7	34.3	0	System Administrator
Yuval Yosha	yosaly	1	03s	<div><div></div></div>	<div><div></div></div>	0	0	0	0	DevOps Engineer
Yishai Gil	yishagi	4	08m 51s	<div><div></div></div>	<div><div></div></div>	3.9	2.3	32.3	0	Group Manager Medi...
Yehiel Zohar	yehielz	2	02m 15s	<div><div></div></div>	<div><div></div></div>	4.3	2	26	0	SW Engineer
Shuly Reichard	ShulyR	9	01h 02m 17s	<div><div></div></div>	<div><div></div></div>	4.1	1.7	21.3	0	DevOps Team Leader
Benjamin Ziv	benjaminz	6	34m 11s	<div><div></div></div>	<div><div></div></div>	4.2	5.2	19.2	0	SW Engineer
Eli Shoval	elish	2	41s	<div><div></div></div>	<div><div></div></div>	4.3	3.5	60	0	DSP Group Manager
Ran Greenberg	rang	3	02m 48s	<div><div></div></div>	<div><div></div></div>	4.3	4.5	7	0	SW Engineer
Glad Moyal	GladM	2		<div><div></div></div>	<div><div></div></div>	0	0	0	0	Customer Support & L...
Roni Pesach	ronip	2	08m 18s	<div><div></div></div>	<div><div></div></div>	0	0	0	0	CAS Leader
Zeev Bodinev	zeevb	2	04m 30s	<div><div></div></div>	<div><div></div></div>	4.3	0.5	12	0	Testing Engineer
Hadas Attal	hadasat	1		<div><div></div></div>	<div><div></div></div>	0	0	0	0	SW Engineer
Naava Sherman	naava	2	07m	<div><div></div></div>	<div><div></div></div>	4.3	0.5	14.5	0	CP Team Leader
Daniel Even-Tzur	daniele	6	18m 21s	<div><div></div></div>	<div><div></div></div>	4.2	1.7	6.7	0	QAM Team Leader
Benny Yossefian	Benny	2	13m 41s	<div><div></div></div>	<div><div></div></div>	3.7	2	3	0	RMA Team Leader

- [Optional] Filter the page to present only information you require. You can filter by Time Range (see [Filtering to Access Specific Information](#) on page 147) or by Users (see [Filtering the User Details Page](#) on page 270).
- Use the following table as reference to the page.

**Table 9-3: Users Experience**

Column	Description
Full Name	The first name and the family name of the end user (the employee) in the enterprise.
User Name	The employee's user name, defined by the enterprise's network administrator.
Calls Count	The total number of calls made by the end user (employee).
Total Duration	The total length of time the end user (enterprise employee) spent on the phone.
Success/Failed	Color-coded bar lets you determine at glance the call success/failure rate (percentage) was for end users. Point your cursor over a specific end user's bar to see the rate of successful versus unsuccessful calls. 
Call Quality	Lets you determine at glance end users calls whose voice quality was measured as Good (green), Fair (yellow) or Poor (red). Point your cursor over a specific end user's bar to see that specific end user's % of calls whose voice quality was measured as Good (green), Fair (yellow) or Poor (red). 
MOS	MOS - Mean Opinion Score (specified by ITU-T recommendation P.800) - the average grade on quality scales of Good to Failed, given by the SEM to voice calls made over a VoIP network at the conclusion of the testing.

Column	Description
Jitter	Jitter (in msec) can result from uneven delays between received voice packets. To space packets evenly, the jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality.
Delay	Delay (or latency) (in msec) - the time it takes for information to travel from source to destination (round-trip time). Sources of delay include voice encoding / decoding, link bandwidth and jitter buffer depth.
Packet Loss	Lost packets, as a percentage - RTP packets that aren't received by the voice endpoint for processing, resulting in distorted voice transmission. Packet Loss can be more than 100%.
Description	The end user's professional position in the enterprise.

4. [Optional] Select an end user's row and then click **Show**; details about that specific user's experience are displayed.
5. [Optional] Click **Refresh** to manually synchronize the page with the Active Directory.

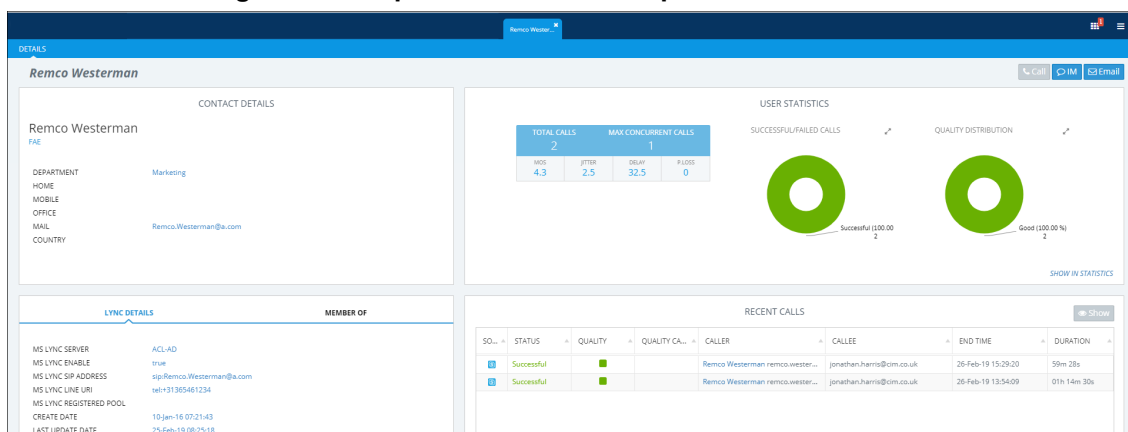
## Assessing a Specific End User's Experience

The OVOC lets operators quickly assess a specific end user's experience, helping operators to tweak the enterprise's telephony network to enhance that experience.

### ➤ To assess a specific end user's experience:

1. Open the Users Experience page (**Users > Users Experience**).
2. Select the row of the end user whose experience you want to assess and then click **Show**; details about this specific end user's experience are displayed.

**Figure 9-7: Specific End User's Experience**



3. Note that the page displaying specific information related to this end user's experience is automatically dynamically tabbed on the menu bar as a pin (labeled **Remco Westerman...** in the page shown above, facilitating quick and easy future access and troubleshooting management. Operators can delete the pin from the menu bar at any time.

## Managing End Users



Only OVOC operators with 'Administrator' security level can perform local management of end users.

Username and passwords of end users are by default locally stored in the OVOC application's database. The User Details page allows operators to locally manage end users. The page mirrors the Active Directory. Any change to the AD is reflected in the User Details page immediately after synchronization is performed.

### ➤ To manage end users:

1. Open the User Details page (**Users > User Details**).

**Figure 9-8: User Details**

USER DETAILS											
<div> <div>USER FILTERS &lt;&lt;</div> <div> <div>Show</div> <div>Refresh</div> </div> </div>											
ADD FILTER											
FULL NAME	USER NAME	DESCRIPTION	DEPARTMENT	OFFICE	MOBILE	HOME	MS LYNC LINE URI	EMAIL	SERVER	COUNTRY	
	RALADS02\$								ACLAD		
	SZADS\$								ACLAD		
	ACLADS01\$								ACLAD		
	DRPADS01\$								ACLAD		
	MVADS01\$								ACLAD		
	BSADS01\$								ACLAD		
	BJADS01\$								ACLAD		
Administrator	root	Built-in account for ad...	IT					root@ac.com	ACLAD		
	SGRODC01\$	SGRODC01\$	Singapore RODO (Om...						ACLAD		
	RALADS01\$								ACLAD		
	ACLADS05\$								ACLAD		
	NLADS01\$								ACLAD		
	AIADS01\$								ACLAD		
	ACLADS03\$	DRP							ACLAD		
	TXADS01\$								ACLAD		
	AIADS04\$								ACLAD		
	ACLADS06\$								ACLAD		
applmgr	applmgr	Oracle Application ser...							ACLAD		
SQL	Sqj	IT							ACLAD		
Adminapc	adminapc								ACLAD		

2. Optionally, use filters for quick access to specific users.
3. Obtain contact information about end users from under the columns in the table: Full Name, User Name, Description, Department, Office, Mobile, Home, MS Skype for Business Line URI, Email, Server, Country.

## Filtering the User Details Page

You can filter the Users Details page using the 'User's filter (click the **Add Filter** button).

**Figure 9-9: Users Filter**

The screenshot shows a vertical filter panel. At the top is a 'TIME RANGE' dropdown with a right-pointing arrow. Below it is a 'USERS' dropdown with a downward-pointing arrow. The main section contains four filter categories, each with a light blue header and a white input area: 'Tenants' (with a dropdown arrow), 'Active directories' (with a dropdown arrow), 'Name' (with a text input field), 'Country' (with a text input field), and 'Department' (with a text input field). At the bottom of the panel is a grey 'APPLY' button.

Use the following table as reference.

**Table 9-4: 'Users' Filter**

Filter	Description
Tenants	From the drop-down, select a configured tenant. Only calls made by and received from users assigned to that tenant will be displayed in the page.
Active directories	From the drop-down, select an Active Directory. Only calls made by and received from users associated with that AD will be displayed in the page.
Name	Enter the name of a user. Only calls made by and received from that user will be displayed in the page.
Country	Enter the name of a country. Only calls made and received by users in that country will be displayed in the page.
Department	Enter the name of a department in the enterprise. Only calls made and received by users in that department will be displayed in the page.

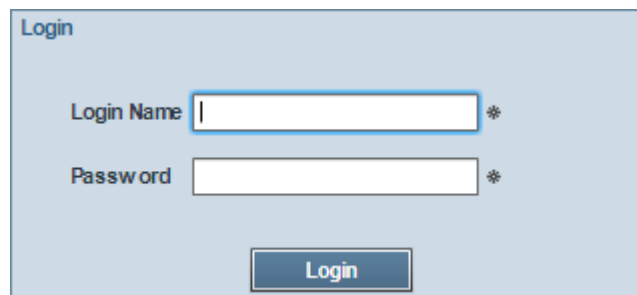
## 10 Producing Reports

The OVOC features essential reports-generation capability that operators can utilize to distribute session experience data and comparative analyses quickly and effectively to responsible persons within the enterprise and to external authorities associated with the enterprise's IP telephony network, for accurate diagnosis and correction of degraded sessions and for general network optimization.

➤ **To open the Reports page:**

- Under the Statistics menu, click the **Reports** tab.

**Figure 10-1: Login**




Log in with the same name and password you used to log in to the OVOC.

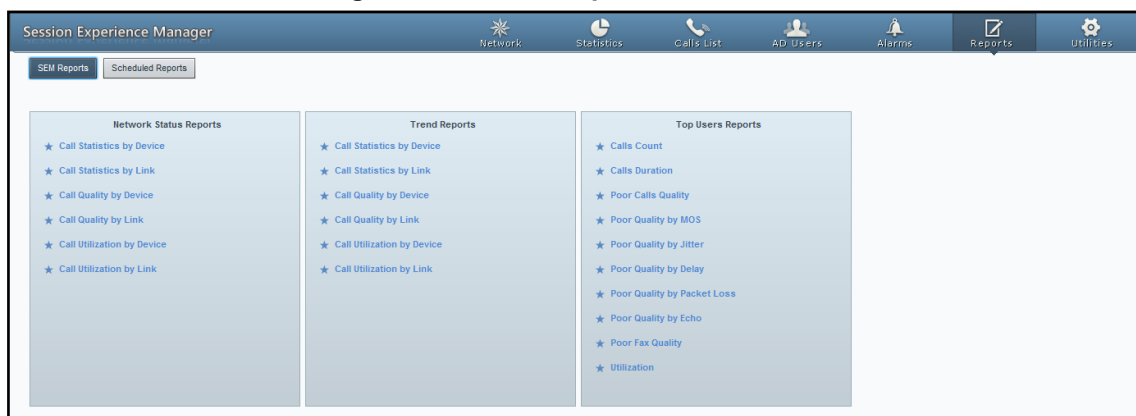
The default name and password are:

**acladmin**

**pass\_1234**

The Session Experience Manager (SEM) Reports module opens.

**Figure 10-2: SEM Reports**




Log in with the same name and password you used to log in to the OVOC.

Three categories of reports help users to quickly and thoroughly analyze different aspects of calls made over the VoIP network:

- Network Status Reports
- Trend Reports
- Top Users Reports

Categories 1 and 2 are identical in terms of the information displayed (columns); however the calculation differs.

Category 1 is calculated as a summary of calls made over the entire period for specified entities (devices / links). The x axis represents the specified entities.

Category 2 is calculated per time interval specified, summarizing the same entity in the specified interval. The x axis represents the time interval (hour / day / week / month).

The following table shows the categories and the reports options in each.











**Table 10-1: Reports Categories**





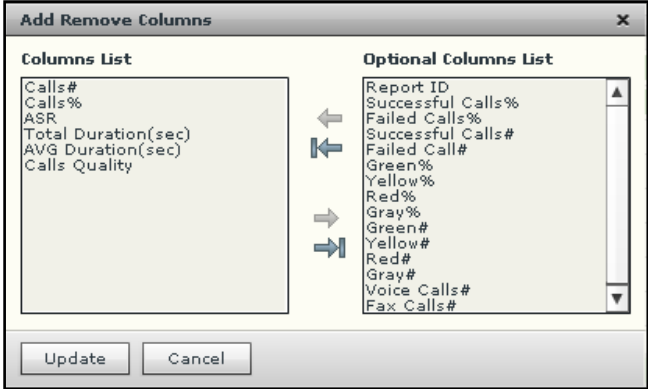
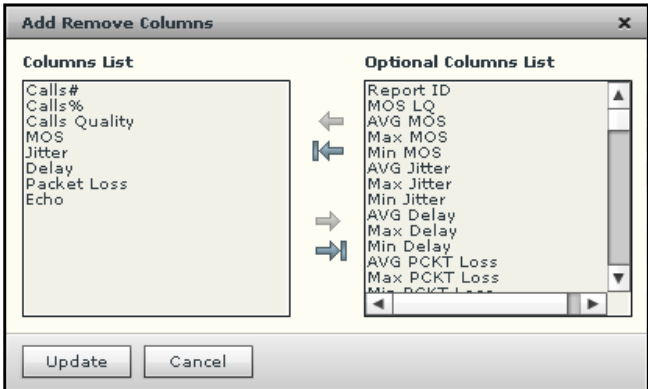
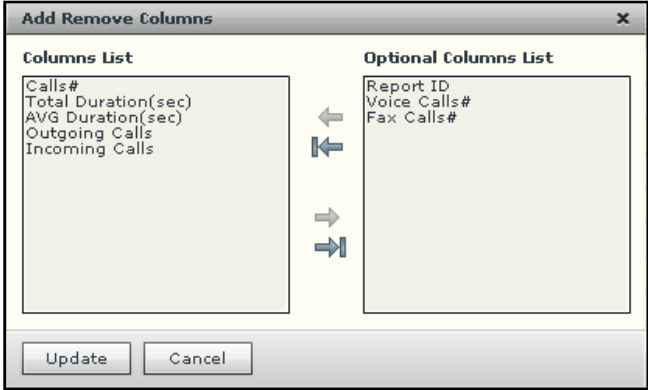
Report Category	Explanation
<b>Network Status Reports</b> <ul style="list-style-type: none"> <li>■ Call Statistics by Device</li> <li>■ Call Statistics by Link</li> <li>■ Call Quality by Device</li> <li>■ Call Quality by Link</li> <li>■ Call Utilization by Device</li> <li>■ Call Utilization by Link</li> </ul>	<p>Displays a summary of key call metrics during a specified time period with a separate row entry for each device/link.</p> <p>Purpose: To compare performance, quality and utilization across devices/links. For example, the 'Call Statistics by Device' report summarizes the % of successful and failed calls and the # of calls that scored in each quality, across specified devices/links. By contrast, a 'Call Quality by Device' report summarizes key metrics affecting voice quality (jitter, delay, packet loss).</p>
<b>Trend Reports</b> <ul style="list-style-type: none"> <li>■ Call Statistics by Device</li> <li>■ Call Statistics by Link</li> <li>■ Call Quality by Device</li> <li>■ Call Quality by Link</li> <li>■ Call Utilization by Device</li> <li>■ Call Utilization by Link</li> </ul>	<p>Displays a summary of key call metrics over specified time intervals of a specified device/link.</p> <p>For example, the 'Calls Trend by Device' report displays 'Number of Calls', 'ASR' and 'Total Duration' in hourly intervals.</p>
<b>Top Users Reports</b> <ul style="list-style-type: none"> <li>■ Calls Count</li> <li>■ Calls Duration</li> <li>■ Poor Calls Quality</li> <li>■ Poor Quality by MOS</li> <li>■ Poor Quality by Jitter</li> <li>■ Poor Quality by Delay</li> <li>■ Poor Quality by Packet Loss</li> <li>■ Poor Quality by Echo</li> <li>■ Poor Fax Quality</li> <li>■ Utilization</li> </ul>	<p>Displays users graded according to number of calls made, calls duration, and calls whose quality scored 'Poor' based on specified metrics.</p>



## Using Reports Features

The following features apply to all reports pages across all three reports categories unless stated otherwise:

Table 10-2: Reports Features

Feature	Description
 Save as CSV	Lets you save a report as a Comma-Separated Value (CSV) file which represents charts, data bars, sparklines, gauges, indicators, etc., in a standardized, plain-text format easily readable and exchangeable with many applications. You can open the file in a spreadsheet such as Microsoft Excel or use it as an import format for other programs.
 Export to PDF	Lets you generate a PDF file of the report reflecting selected filters, columns, graphs, etc.
Filters	Let you specify: <ul style="list-style-type: none"> <li>■ The Time Range for the report to cover (in the Network Status Reports page)</li> <li>■ The Time Range and the Interval for the report to cover (in the Trend Report page; Hourly, Daily, Weekly or Monthly)</li> <li>■ Devices / Links on which to produce the report</li> <li>■ Top 10/20/30 Users on which to produce the report (in the Top Users Report page)</li> </ul>
SEM Reports	Click the button at any time to return to the Reports page displaying the three reports categories and the report options available under each. Click an option to produce a report.
Scheduled Reports	Click the button to schedule a report.
	Displayed after selecting a report to produce in the reports menu. First filter (see above) and then click it; the report is produced and displayed.
Charts view / Table view	Two views are displayed in every report produced: Charts (uppermost) and table (lowermost). Click  to expand charts view; table view is eclipsed. Click  to revert to both views.
Switch to horizontal / Switch to vertical	Charts are by default displayed vertically, one below the other, in this order: Calls #, Calls %, ASR, Total Duration, AVG Duration and Calls Quality. Use the scrollbar to scroll down from one to the next. They can optionally be displayed horizontally to suit user preference. To display horizontally, click the link. Click next  or previous  to navigate from chart to chart.
 Bar /  Linear	[Only applies to Network Status Reports] By default, charts are displayed as bar charts. Click the drop-down to choose linear charts if required.
 Add / Remove Columns	Click the icon; optional table view columns are displayed.

Feature	Description
	<p>To add, if required, select an optional column and click  or select all and click . To remove a column, select it in the Columns List pane and click  or select all and click .</p> <p>Default metrics columns (left pane) and optional metrics columns (right pane) in the Summary/Trend category (except 'Call Quality by Device / Link') are as follows:</p>  <p>Default metrics columns (left pane) and optional metrics columns (right pane) in a 'Call Quality by Device / Link' report in the Summary/Trend category are:</p>  <p>Default metrics columns (left pane) and optional metrics columns (right pane) in the Top Users reports category are:</p> 

Feature	Description
	See in <a href="#">Producing Top Users Reports</a> on page 280 for variations across reports in the Top Users Reports category.
 Show Column Graphical Representation Display column as chart	Table column headers display this icon. Click one to display the metric as a chart. If the chart is already open, you're notified. After report generation, the table's ASR metric column is the only one displayed as a chart in Charts view.
Table Bottom Line (Total)	The table's bottom line shows column's total. For example: <ul style="list-style-type: none"> <li>■ Calls # column's bottom line shows the total sum of all counts of all calls on all devices / links</li> <li>■ ASR column's bottom line shows the average success rate of the average success rates of all devices / links.</li> </ul> 'Total' is calculated according to the measured parameter. It can be SUM, AVG, MIN or MAX.
Search 	Users can use the 'Search' option to search for and find precise information related to a query. When information related to the search query is found, the report exclusively displays only that information.

## Producing a Network Status Report

Network Status Reports show the sum totals, over the entire period, of calls performance scores, quality scores, #s, %s, total duration and average duration (default metrics). Reports in this category are identical in terms of metrics measured. Metrics columns can optionally be added / removed (see 'Add / Remove Columns' in the table in [Using Reports Features](#) on page 272).

### ➤ To produce a Network Status Report:

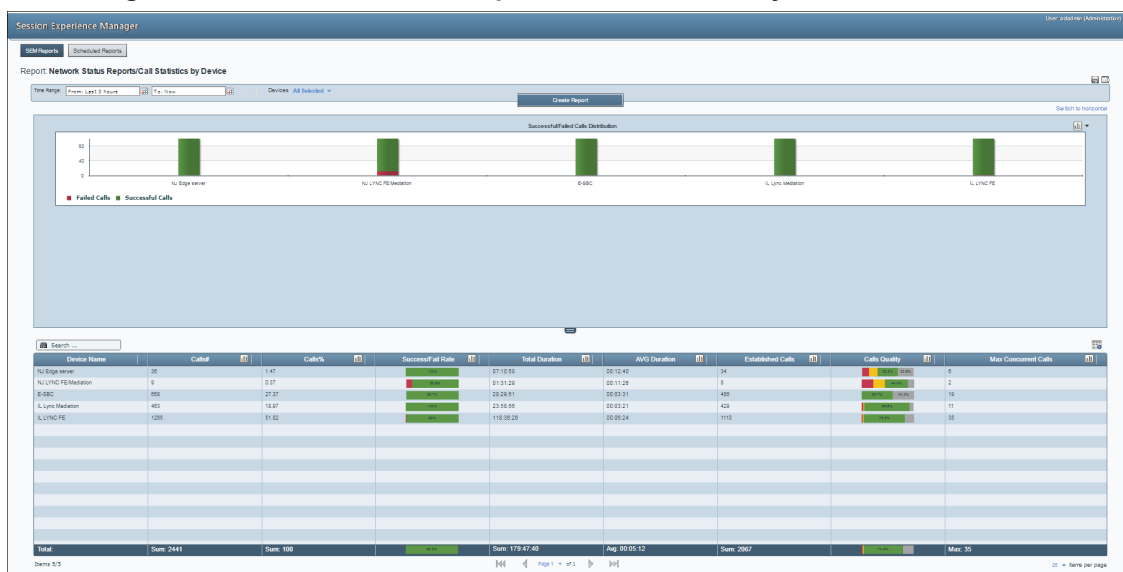
1. Click an option in the 'Network Status Reports' category, for example, click the first option, i.e., Call Statistics by Device.

**Figure 10-3: Create Report**



2. Filter for 'Time Range' and 'Devices'.
3. Click the **Create Report** button:

Figure 10-4: Network Status Report – Call Statistics by Device



Following report generation, the Success/Fail Rate column is the only one displayed in charts view.

### ➤ To display a metric as a chart:



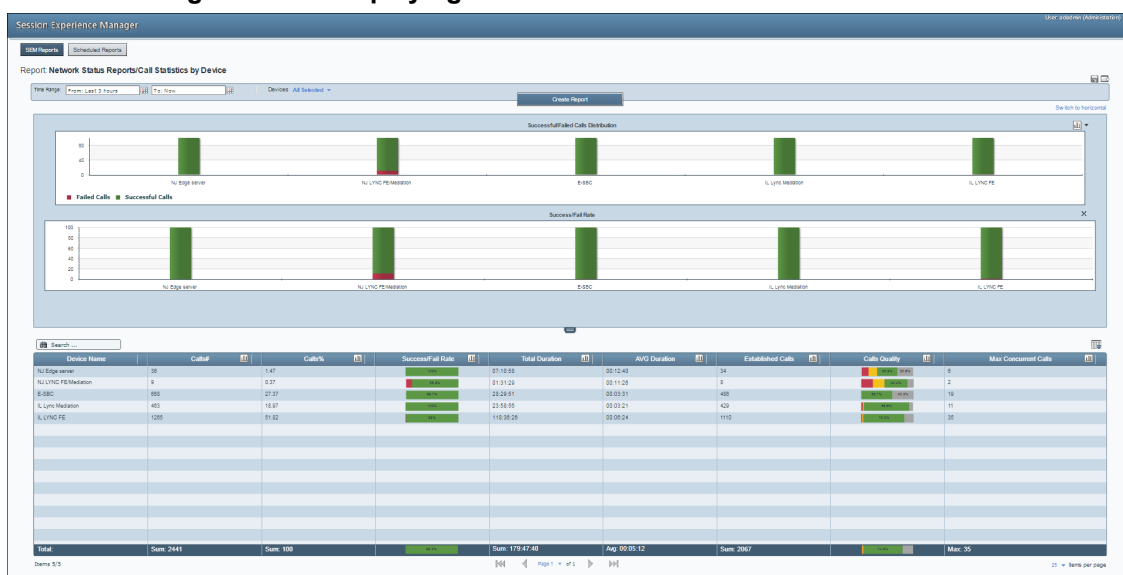




- In the table, click  in the metric's column header. For example, click  in the Success/Fail Rate column header; the Success/Fail Rate chart is displayed:

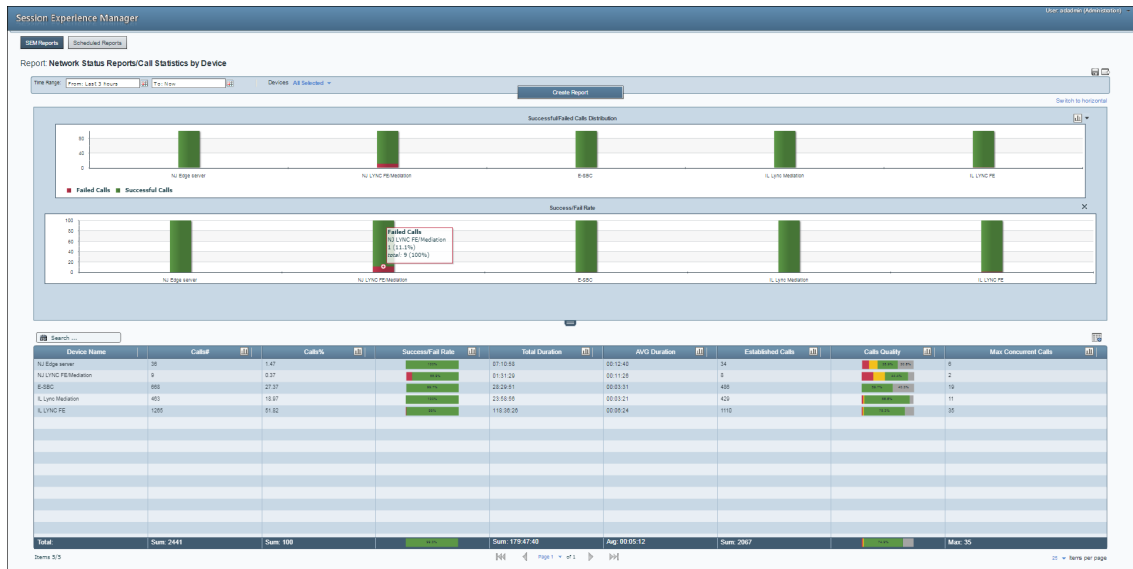
Figure 10-5: Displaying the Success/Fail Rate Chart



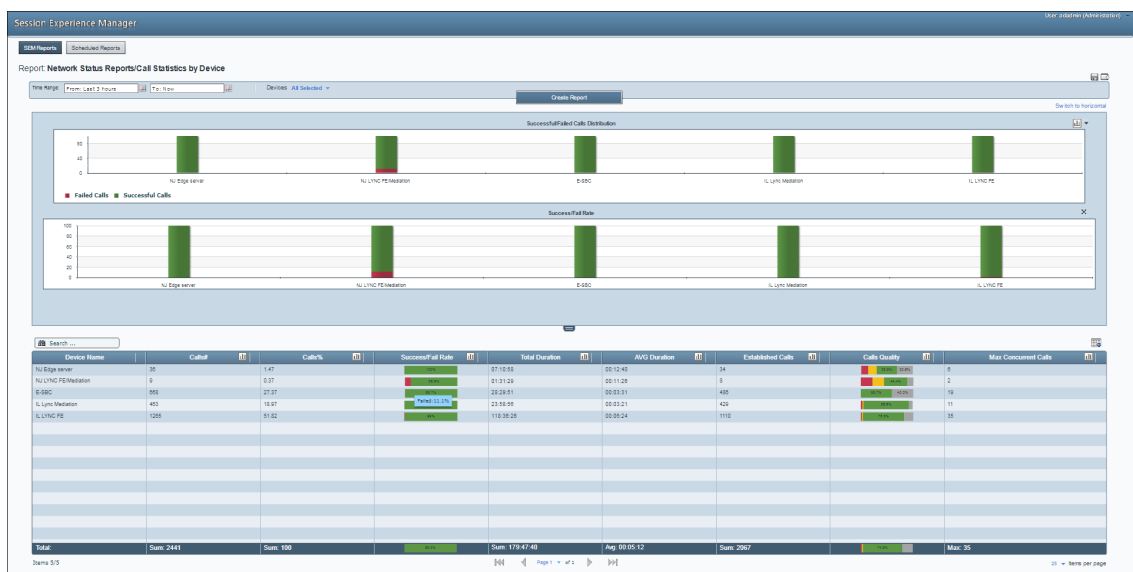
In a Network Status Report you can:

- Click the **Switch to horizontal** link to switch from vertical view (default) to horizontal view.
- Click  to expand the charts pane. Click it again to contract it.
- Click  to switch from bar charts (default) to linear charts. Select  from the drop-down (see 'Charts view / Table view' in the table in [Using Reports Features](#) on page 272).
- Click  to add/remove a column to/from the table (see 'Add / Remove Columns' in the table in [Using Reports Features](#) on page 272).
- See in the chart which entities registered the highest failed / successful calls rate.

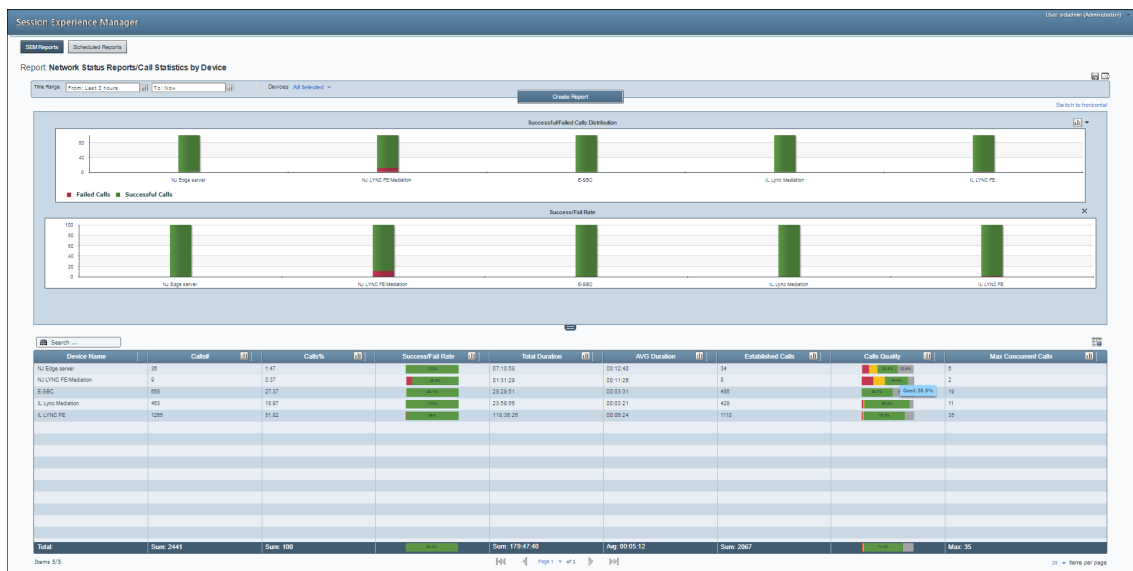
- See in the table on which entities most calls were made, what % of calls were made on each, on which entities most failed / successful calls were made, on which entities most call time was recorded, on which entities the average call duration was longest / shortest and on which entity voice quality scored highest (green = good, yellow = fair, red = poor, grey = unknown).
- See in the chart an entity's success / fail rate (%). Point your cursor over a color in a bar (green = successful, red = failed):



- See in the table an entity's success / fail rate (%). Point your cursor over the entity's row (green = successful, red = failed):



- See in the table quality scores by pointing your cursor over a color in the entity's Calls Quality row (green = good, yellow = fair, red = poor, grey = unknown):



Default and optional table columns in Network Status Reports are:

**Table 10-3: Table Columns in Network Status Reports**

Network Status Report Type	Default Columns	Optional Columns
Call Statistics by Device	Name, Calls #, Calls %, Success/Fail Rate, Total Duration, AVG Duration, Established Calls, Calls Quality, Max Concurrent Calls	Report ID Successful/Failed Calls % Successful/Failed Calls # Good/Fair/Poor/Unknown % Good/Fair/Poor/Unknown # Voice Calls # Fax Calls # Total Duration AVG Duration
Call Quality by Device	Name, Voice Calls #, Calls %, Calls Quality, MOS, Jitter, Delay, Packet Loss, Echo	Report ID AVG/Max/Min MOS/Jitter/Delay/Package Loss/Echo AVG SNR Good/Fair/Poor/Unknown % Good/Fair/Poor/Unknown # MOS/Jitter/Delay/Package Loss/Echo Good/Fair/Poor/Unknown % MOS Calls # Jitter Calls # Delay Calls #

Network Status Report Type	Default Columns	Optional Columns
		Packet Loss Calls # Echo Calls # SNR Calls #
Call Utilization by Device	Name AVG Total Kbps AVG Rx Kbps AVG Tx Kbps AVG Packet Loss	Report ID Calls # Packet Loss Calls #



The table above shows call statistics, quality and utilization *by device*. The same default and optional columns apply to call statistics, quality and utilization *bylinks*, but in terms of *streams* rather than *calls*.


- You can re-filter and re-run the report (see 'Filters' in the table in [Using Reports Features](#) on page 272).
- You can generate another report. Click the SEM Reports button.
- You can schedule a report. Click the Scheduled Reports button (for details see [Scheduling a Report](#) on page 282).

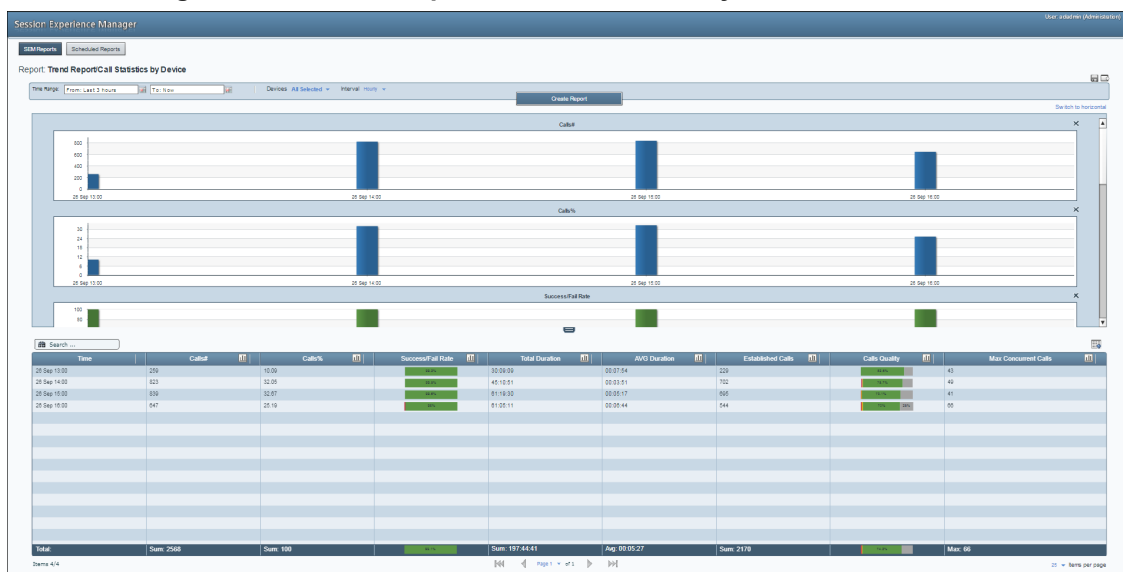
## Producing Trend Reports

Trend reports show general tendencies over intervals of calls performance, quality, #s, %s, total duration and average duration (default metrics measured).







Reports in this category are identical in terms of metrics columns displayed. Columns can optionally be added / removed (see 'Add / Remove Columns' in the table in [Using Reports Features](#) on page 272).

### ➤ To produce a trend report:

1. Click an option in the 'Trend Reports' category, e.g., the first; the 'Run now'  page opens
2. Filter for 'Time Range' and 'Devices'. For the 'Interval' filter select Hourly, Daily, Weekly or Monthly.
3. Click **Create Report**.

**Figure 10-6: Trend Reports – Call Statistics by Device**

In a Trend Report you can:


- See when most/least calls were made, how many, % of total, each period's success/fail rate and each period's quality scores.
- Click the Switch to horizontal link to switch from vertically viewed charts (default) to horizontally viewed charts (see the table in [Using Reports Features](#) on page 272).
- Click  to switch from bar (default) to linear charts. Select  from the drop-down (see 'Charts view / Table view' in the table in [Using Reports Features](#) on page 272).
- Click  in a column header in the table to display that column as a chart (see 'Show Column Graphical Representation' in the table in [Using Reports Features](#) on page 272)
- Click  to add a column to table view or remove a column from table view (see 'Add / Remove Columns' in the table in [Using Reports Features](#) on page 272). Default columns and optional columns are identical to the 'Call Statistics by Device/Link' and 'Call Quality by Device/Link' reports in the Network Status Reports category.
- Use the pager to navigate to a page if there are multiple pages.
- Re-filter and re-run the report (see 'Filters' in the table in [Using Reports Features](#) on page 272)
- Export the report to PDF. Click  (see 'Export...' in the table in [Using Reports Features](#) on page 272)
- Save the report as a CSV file. Click  (see 'Save...' in the table in [Using Reports Features](#) on page 272)
- Choose to produce another report by clicking the SEM Reports button.

## Producing Top Users Reports

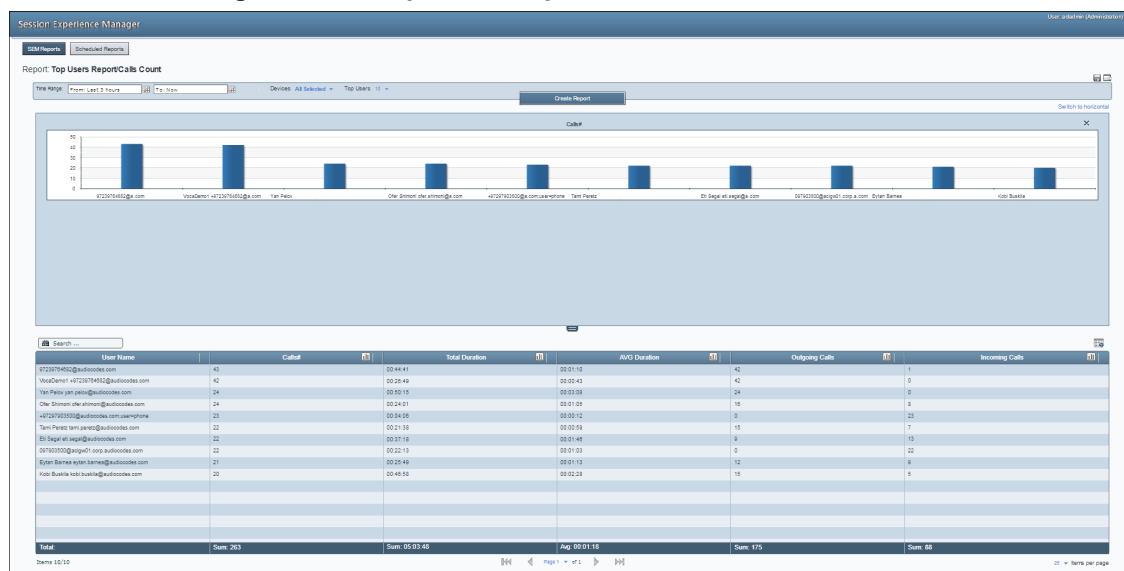
Top Users reports display the top 10, 20 or 30 users in terms of # of calls made, total duration, average duration, outgoing calls and incoming calls (default metrics measured).

Reports in this report category are identical in terms of metrics columns displayed. Metrics columns can optionally be added / removed (see 'Add / Remove Columns' in the table in [Using Reports Features](#) on page 272).





➤ **To produce a top users report:**

1. Click an option in the 'Top Users Reports' category, for example, click the first report option, i.e., Calls Count; the 'Run now'  page opens.
2. Filter for 'Time Range' and 'Devices'. For the 'Top Users' filter, select 10, 20 or 30.
3. Click **Create Report**.

**Figure 10-7: Top Users Report – Calls Count**



In a Top Users Report you can:

- Save the report as a CSV file. Click  (see 'Save...' in the table in [Using Reports Features](#) on page 272)
- Export the report to PDF. Click  (see 'Export...' in the table in [Using Reports Features](#) on page 272)
- Click the **Switch to horizontal** link to switch from vertically viewed charts (default) to horizontally viewed charts (see the table in [Using Reports Features](#) on page 272)
- Click  in a column header in the table to display that column as a chart (see 'Show Column Graphical Representation' in the table in [Using Reports Features](#) on page 272)
- Click  to add a column to table view or remove a column from table view (see 'Add / Remove Columns' in the table in [Using Reports Features](#) on page 272).

Default and optional table columns in Top Users reports are:

**Table 10-4: Table Columns in Top Users Reports**

Top Users Report Type	Default Columns	Optional Columns
Calls Count	User Name, Calls #, Total Duration, Average Duration, Outgoing Calls, Incoming Calls	Report ID, Voice Calls #/Fax Calls #, Total Duration (sec), AVG Duration (sec)
Calls Duration	User Name, Total Duration, Calls #, Average Duration, Outgoing Calls, Incoming Calls	Report ID, Total Duration (sec), AVG Duration (sec)
Poor Calls Quality	User Name, Poor Quality Calls, Calls #, Calls Quality	Report ID

Top Users Report Type	Default Columns	Optional Columns
		Unknown / Good / Fair / Poor % Fair # Poor #
Poor Quality by MOS / Jitter / Delay / Packet Loss / Echo	User Name, AVG MOS / Jitter / Delay / Packet Loss / Echo, Calls #, Total Duration	Report ID MOS / Jitter / Delay / Packet Loss / Echo Calls # Total Duration (sec)
Poor Fax Quality	User Name, Poor Quality Faxes, Poor Quality Pages, Total Faxes, Total Pages	Report ID
Utilization	User Name, Total, RX, TX	Report ID

- Use the pager to navigate if there are multiple report pages.
- Re-filter and re-run the report (see 'Filters' in the table in [Using Reports Features](#) on page 272)
- Choose to produce another report by clicking the **SEM Reports** button.

## Scheduling a Report

You can schedule the SEM to automatically produce a report periodically.

### ➤ To schedule a report:

1. Click the Reports icon; the SEM Reports page opens (see the table in [Using Reports Features](#) on page 272).
2. Click the **Scheduled Reports** button.

**Figure 10-8: Scheduled Reports**

Report Name	Report Topic	Report Group	Schedule Name	Description	Scheduling Frequency	Num to Run	Num of Run Times	Reports	User	Last Run Time	Next Run Time	Forward Mail Addresses
Call Statistics by Device	Network Status Rep	SEM Report	Call_Stat	Test	Hourly	1	1	Successful	ovmp	21:20:00 Jan 23		ovmp@n.com
Call Statistics by Device	Network Status Rep	SEM Report	Test		Weekly	1	4	Successful	ovmp	00:00:00 Feb 10	00:00:00 Mar 09	ovmp@n.com

3. Click  to add a schedule.

Figure 10-9: Scheduler

The screenshot shows a 'Scheduler' dialog box with the following sections and controls:

- Scheduler Main Settings:**
  - Report Name:** A dropdown menu currently showing 'Call Statistics by Device'.
  - Scheduler Name:** An empty text input field.
  - Description:** An empty text input field.
- Report Filter Settings:**
  - Devices:** A dropdown menu showing 'All Selected' with a downward arrow.
- Scheduler Settings:**
  - Frequency:** Four radio buttons for 'Hourly', 'Daily' (selected), 'Weekly', and 'Monthly'.
  - Selected daily report generation, set day time (Server Timezone):**
    - Generate report at:** Two spinners for 'Hours' (set to 0) and 'Minutes' (set to 0).
    - Run Report:** Two radio buttons: 'No End' (selected) and 'Run'.
    - Run Times:** A spinner set to '1' followed by the text 'times'.
- Mail Settings:**
  - Forward to Mail:** An unchecked checkbox.
  - Mail Addresses (:):** An empty text input field.

At the bottom right are 'OK' and 'Cancel' buttons.

4. Under 'Report Name', select a report to schedule from the 'Report' drop-down list. All reports under all three report types are listed.
5. In the 'Scheduler Name' field define a name to help you easily identify the schedule.
6. In the 'Description' field, provide a description to help you distinguish this schedule from others.
7. Under 'Report Filter' you can filter the devices on which the report which you're scheduling will be produced. By default, all devices will be included. Click **All Selected** to change the default. For detailed information on how to filter devices, see [Filtering by 'Status'](#) on page 152.
8. Under 'Report Frequency', select either **Hourly**, **Daily** (default), **Weekly** or **Monthly**. If the frequency you select is **Daily**, set the 'Time'.
9. Under 'Run Times', select Unlimited or Limit to limit the schedule to a limited number of report run times (you can limit to up to 100 run times).
10. Under 'Forward Report', select the Mail option for the report to be automatically forwarded to your email address.
11. In the 'Mail Addresses' field, define the email address / addresses to which to automatically forward the report.
12. Click **OK**; the report is scheduled; you can expect the first to arrive in your mail according to schedule.

## Viewing a Scheduler Generated Report

You can view a report generated by the scheduler.

### ➤ To view a report generated by the scheduler:

1. In the Scheduled Reports page under the Reports column, click the **Generated** hyperlink in the row of the report generated by the scheduler; the Report Generated by Scheduler opens.

**Figure 10-10: Report Generated by Scheduler**


Report Name	Report Type	Report Group	Schedule Name	Description	Scheduling Frequency	Run to Run	Run of Run Times	Generated Reports	User	Last Run Time	Next Run Time	Forward Mail Addresses
Call Statistics by Device	Network Status Page	SEM Reports	BEST		Hourly		5	2024	admin		2024-02-26 00:00:00	

2. Click **Show**; the report is generated according to the scheduler.

## Saving the File of a Scheduler Generated Report

You can save the file of a report generated by the scheduler.


### ➤ To save the file:

1. In the Report Generated by Scheduler, click  Save Report File.
2. Select the location on your pc in which to save the file and click Save.

## Deleting the File of a Scheduler Generated Report

You can delete the file of a report generated by the scheduler.


### ➤ To delete the file:

1. In the Report Generated by Scheduler page, click  Delete File; you're prompted 'Delete Generated Report File?'
2. Click **Yes**; the file is deleted.

## Editing a Schedule

You can edit a report schedule.

### ➤ To edit a schedule:

1. In the Scheduled Reports page, click  Update Scheduler; the Scheduler opens.
2. Edit the reports schedule and then click **OK**; you're prompted *Previous attachments will be deleted. Are you sure you want to continue?*
3. Click **Yes**; the edited schedule is displayed in the Scheduled Reports page.

## Deleting a Schedule

You can delete a report schedule.

### ➤ To delete a schedule:

1. In the Scheduled Reports page, click  Delete Scheduler; you're prompted 'Are you sure?'
2. Click **Yes**; the report schedule is deleted.

## Manually Running or Pausing a Schedule

You can manually run or pause a report schedule.

➤ **To manually run a schedule:**

- In the Scheduled Reports page, click  Run Scheduler; the icon changes to  and the report scheduler is run.









➤ **To manually pause a schedule:**

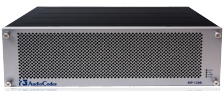
- Click  Pause Scheduler; the icon reverts to  and the scheduler is paused.


# 11 AudioCodes IP Network Telephony Equipment





The following table shows the supported AudioCodes IP network telephony equipment.


**Table 11-1: Supported AudioCodes IP Network Telephony Equipment**

Supported IP Network Telephony Equipment	Description
 <p>MediaPack</p>	<p><b>MP-1xx:</b> Analog VoIP devices featuring up to 24 analog ports connected directly to an enterprise PBX (FXO), to phones, or to fax (FXS). Support up to 24 simultaneous calls.</p> <p><b>MP-20x:</b> VoIP Gateway. An all-in-one unit featuring (depending on model) a VoIP adapter, FXS lines, FXO interfaces, Ethernet LAN interfaces (with an internal Layer-2 switch), and Ethernet WAN interface.</p> <p>(See product documentation for detailed information)</p>
 <p>Mediant 500 E-SBC</p>  <p>Mediant 500L E-SBC</p>	<p>Members of the AudioCodes family of Enterprise Session Border Controllers. Enable connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. Provide VoIP SBC functionality. Offer enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.</p>
 <p>Mediant 500 MSBR</p>  <p>Mediant 500L MSBR</p>  <p>Mediant 800 MSBR</p>  <p>Mediant 1000 MSBR</p>	<p>These Multi-Service Business Routers are networking devices that combine multiple service functions such as a Media Gateway, Session Border Controller (SBC), Data Router and Firewall, LAN switch, WAN access, Stand Alone Survivability (SAS) and an integrated general-purpose server.</p> <p>Stand Alone Survivability (SAS) functionality offers service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. SAS enables internal office communication between SIP clients, along with PSTN fallback in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX.</p> <p>The devices also provide an integrated Open Solution Network (OSN) Server module. The OSN can host a variety of third-party applications such as IP-PBX, Call Center, and Conferencing.</p> <p>(See the specific product documentation for detailed information)</p>
 <p>Mediant 500 Enterprise Session Border Controller (E-SBC)</p>	<p>Member of the AudioCodes family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. Provides VoIP SBC functionality. Offers enhanced dialing plans and voice routing capabilities along with SIP-to-SIP mediation, allowing enterprises to implement SIP Trunking services (IP-to-IP call routing) and IP-based Unified Communications.</p>

Supported IP Network Telephony Equipment	Description
 Mediant 2600 E-SBC	<p>Member of the AudioCodes family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. The device is a fully featured enterprise-class SBC that provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation. The SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.</p>
 AudioCodes Mediant Software Enterprise Session Border Controllers	<p>Mediant Software E-SBCs are pure-software products, enabling connectivity and security between enterprises' and service providers' VoIP networks. Includes the following product variants:</p> <p><b>Mediant Server Edition SBC:</b> x86 server-based platform, which must be installed on a server that complies to the specified hardware requirements.</p> <p><b>Mediant Virtual Edition SBC:</b> Installed and hosted in a virtual machine environment that complies to specified requirements.</p>
Mediant Cloud Edition	<p>The OVOC supports the AudioCodes Mediant Cloud Edition. The feature is offered by the Mediant VE SBC in AWS-based environments. It provides similar functionality to the Media Transcoding Cluster feature but is in the cloud, and its Media Components handle transcoding as well as all media directly, without traversing the Mediant VE SBC.</p>
 MP-1288	<p>Cost-effective best-of-breed, high density analog media VoIP gateway. Provides superior voice technology for connecting legacy telephones, fax machines and modems with IP-based telephony networks, as well as for integration with IP PBX systems. Designed and tested to be fully interoperable with leading soft switches, unified communications (UC) servers and SIP proxies.</p> <p>Designed for carrier environments including 1+1 power supplies and 1+1 Ethernet redundancy, maintaining high voice quality to deliver reliable enterprise VoIP communications. Advanced call routing mechanisms, network voice quality monitoring and survivability capabilities (including PSTN fallback) result in minimum communications downtime.</p>
 Mediant 3000 Media Gateway	<p>Medium-sized member of the family of market-ready, standards-compliant Media Gateway systems.</p>

Supported IP Network Telephony Equipment	Description
	<p>Main features: Redundant common equipment (Power, Controller, Ethernet Switch); Optional N+1 protection of DSP Cards; Designed for NEBS Level 3; Optimal, cost-effective channel density; Field-proven, high voice quality; SS7/SIGTRAN Interworking (SS7/PRI); Open, scalable architecture; Flexible deployment options; Packet telephony standards-compliant; IETF and ETSI standards-compliant</p> <p>Applications: VoP Trunking devices, IP-Centrex devices, VoP Access devices</p> <p>Selected specifications: Up to 2,880 independent VoIP to PSTN voice calls; Voice Coders: include G.711, G.723.1, G.726, G.728, G.729A; G.165 and G.168 compliant echo cancellation; T.38 compliant relay or fallback to G.711 analog fax and modem support; call progress tones, VAD, CNG, dynamic programmable jitter buffer, modem detection, DTMF detection and generation. Signaling: PSTN: ISDN PRI, CAS, MFC-R2, MF-R1, SS7/M2UA/SIGTRAN Interworking, IP Transport: IETF RFC 1889, RFC 1890 RTP/IP Transport, TCP, UDP (See product documentation for detailed information)</p>
 Mediant 4000 E-SBC	<p>Member of the AudioCodes family of E-SBCs. Enables connectivity and security between small medium businesses (SMBs) and service providers' VoIP networks. The device is a fully featured enterprise-class SBC provides a secured voice network deployment based on a Back-to-Back User Agent (B2BUA) implementation. SBC functionality provides perimeter defense for protecting the enterprise from malicious VoIP attacks; mediation for allowing the connection of any IP PBX to any service provider; and service assurance for service quality and manageability.</p>
 Mediant 9000 SBC	<p>Highly scalable Session Border Controller designed for deployment in large enterprise and contact center locations and as an access SBC for service provider environments. High-capacity SBC supporting thousands of concurrent sessions and extensive SIP connectivity with wide-ranging interoperability, enhanced perimeter defense against cyber-attacks, and advanced voice quality monitoring.</p> <p>Also supports active/standby (1+1) redundancy (High Availability) by employing two devices in the network. Offers branch survivability during WAN failure, ensuring call service continuity.</p>
<p>Survivable Branch Appliance (SBA)</p> 	<p>Designed for Microsoft Skype for Business Server, the Survivable Branch Appliance (SBA) allows remote branch resiliency in a Microsoft Skype for Business Server network. The AudioCodes SBA resides on the OSN server platform of the Mediant 800B and the Mediant 1000B running on a Microsoft Windows 2008 Telco R2 operating system.</p> <p>Displayed in the OVOC as a module of the Mediant 800B and the Mediant 1000B devices. When you add either of these platforms to the OVOC, there is an option to enable the SBA module. The SBA module has a separate IP address and FQDN Name.</p>

Supported IP Network Telephony Equipment	Description
	<p>405HD, 420HD, 430HD, 440HD (shown here), 445HD, 450HD and C450HD IP phones, based on AudioCodes High Definition voice technology, providing clarity and a rich audio experience in VoIP calls. All models include a large monochrome multi-language graphic LCD display. The phones provide voice communication over an IP network, allowing you to place and receive phone calls, put calls on hold, transfer calls, make conference calls, etc. Phone models support Microsoft Skype for Business environments as well as non-Microsoft environments.</p>
	<ul style="list-style-type: none"> <li>■ CloudBond 365 is a modular, adaptable solution for the data center, customer premises or the branch. A versatile all-in-one Skype for Business appliance designed for hybrid environments, it combines the best of the Skype for Business server, the Cloud-PBX and the service provider's voice services.</li> <li>■ User Management Pack (UMP) 365 is a software application for managing Skype for Business users on premises or in Cloud PBX environment and is also part of the AudioCodes CloudBond 365 solution and applies to all CloudBond 365 editions - Standard, Standard+, Pro, Enterprise and Virtualized Edition.</li> </ul>
SmartTAP	<p>The AudioCodes SmartTAP 360° Recording for Microsoft Skype for Business is an intelligent, fully certified and secured enterprise interactions recording solution of voice, video and IMs. With SmartTAP, enterprises can capture and index any customer or organizational interaction across external and internal communication channels seamlessly.</p>
	<p>The AudioCodes Mediant Server CCE Appliance bundles AudioCodes field-proven SBCs and gateways with the Skype for Business Cloud Connector Edition into an elegantly packaged 1U chassis that is easy to deploy and manage.</p> <p>Based on a powerful HP server, the Mediant Server CCE Appliance delivers the Cloud Connector integrated with the AudioCodes SBC for organizations or enterprise branches with up to 2500 users and supports up to 500 concurrent sessions.</p>
	<p>The AudioCodes Mediant 800 CCE Appliance bundles AudioCodes field-proven SBCs and gateways with the Skype for Business Cloud Connector Edition into an elegantly packaged 1U chassis that is easy to deploy and manage.</p> <p>For organizations or enterprise branches with up to 1000 users, the AudioCodes Mediant 800 with the integrated OSN server module can host the Cloud Connector on the same self-contained appliance supporting up to 185 concurrent sessions.</p>

Supported IP Network Telephony Equipment	Description
 The logo for Voice.AI Gateway is a blue rounded square. Inside, there is a white graphic of a sound wave with five vertical bars of increasing height from left to right. To the right of the graphic, the text "Voice.AI" is written in white, with "Gateway" in a smaller font size below it.	<p>The AudioCodes Voice.AI Gateway brings an intuitive form of human communications to an enterprise's chatbot service. Supporting phone and WebRTC voice calls, the service eliminates waiting time, increases caller satisfaction and can save up to 30% in support expenditure by automating simple and repetitive tasks.</p>

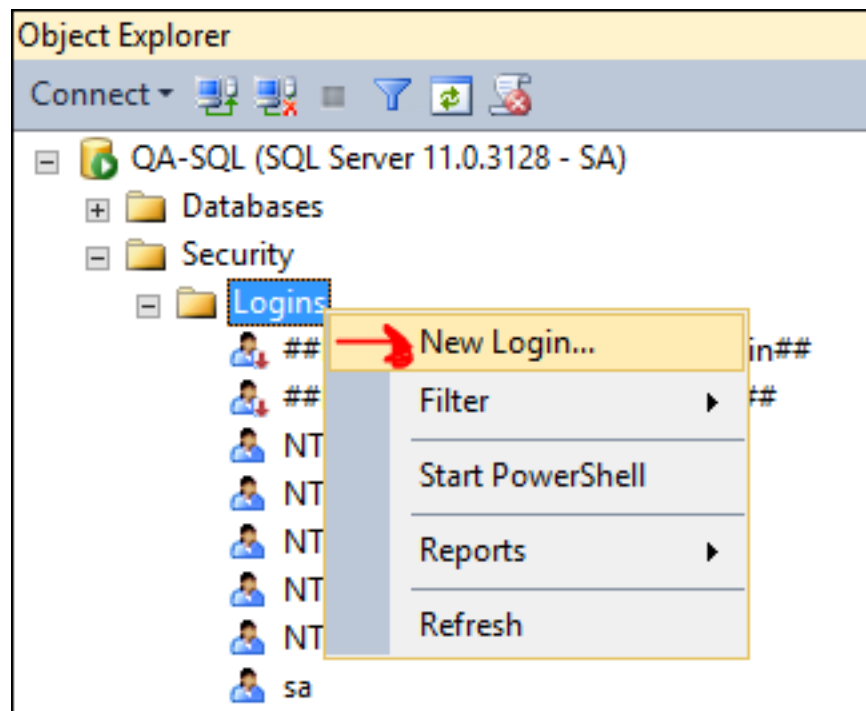
## 12 Adding an Unprivileged User to MSSQL Server

An unprivileged user can be added to the MSSQL server with SQL Server Management Studio.

➤ To add an unprivileged user to the MSSQL server:

1. In the 'Security' folder, right-click **Logins** and select **New Login**.

Figure 12-1: New Login



2. Under 'General', enter the Login name, select the **SQL server authentication** option, enter and confirm the password, from the 'Default database' drop-down select the default database to log in with, and then click **OK**.

Figure 12-2: SQL Server Authentication

Login - New

Select a page: General, Server Roles, User Mapping, Securables, Status

Script Help

Login name: Sem12

Windows authentication

SQL Server authentication

Password: .....

Confirm password: .....

☐ Specify old password

Old password: .....

☒ Enforce password policy

☒ Enforce password expiration

☒ User must change password at next login

☐ Mapped to certificate

☐ Mapped to asymmetric key

☐ Map to Credential

Mapped Credentials

Credential	Provider
------------	----------

Default database: LcsCDR

Default language: <default>

Progress: Ready

OK Cancel

3. Under 'Server Roles' shown in the following figure, select **public**.

Figure 12-3: Login Properties – Servers Role - public

Login - New

Select a page: General, Server Roles, User Mapping, Securables, Status

Script Help

Server role is used to grant server-wide security privileges to a user.

Server roles:

- ☐ bulkadmin
- ☐ dbcreator
- ☐ diskadmin
- ☐ processadmin
- ☒ public
- ☐ securityadmin
- ☐ serveradmin
- ☐ setupadmin
- ☐ sysadmin

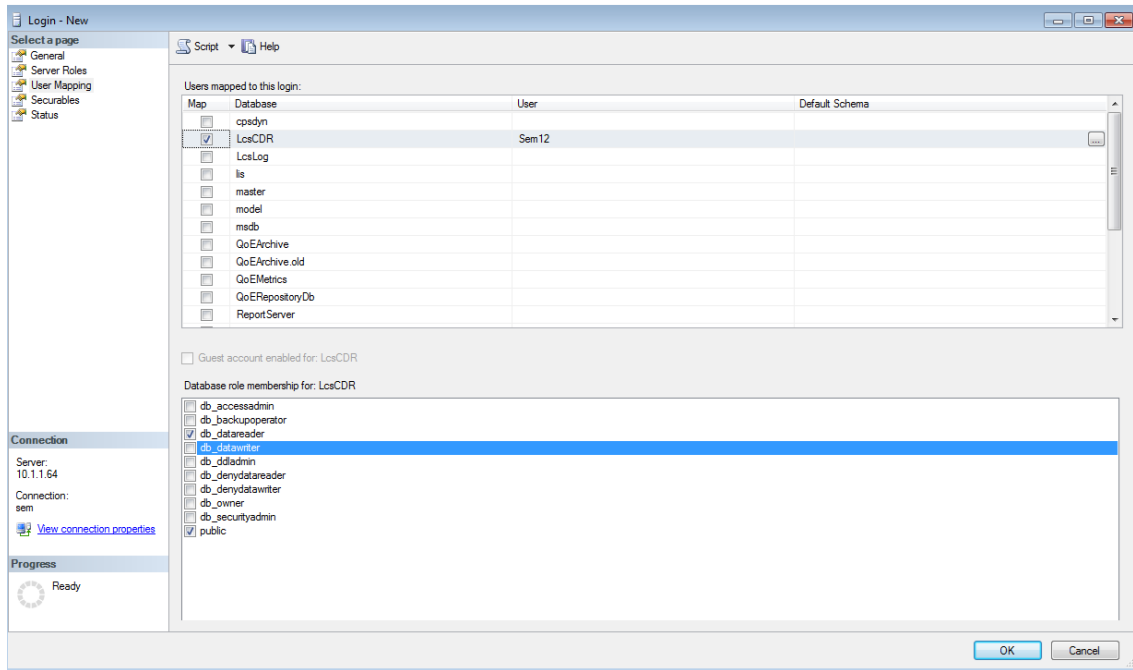
Connection

Server: QA-SQL

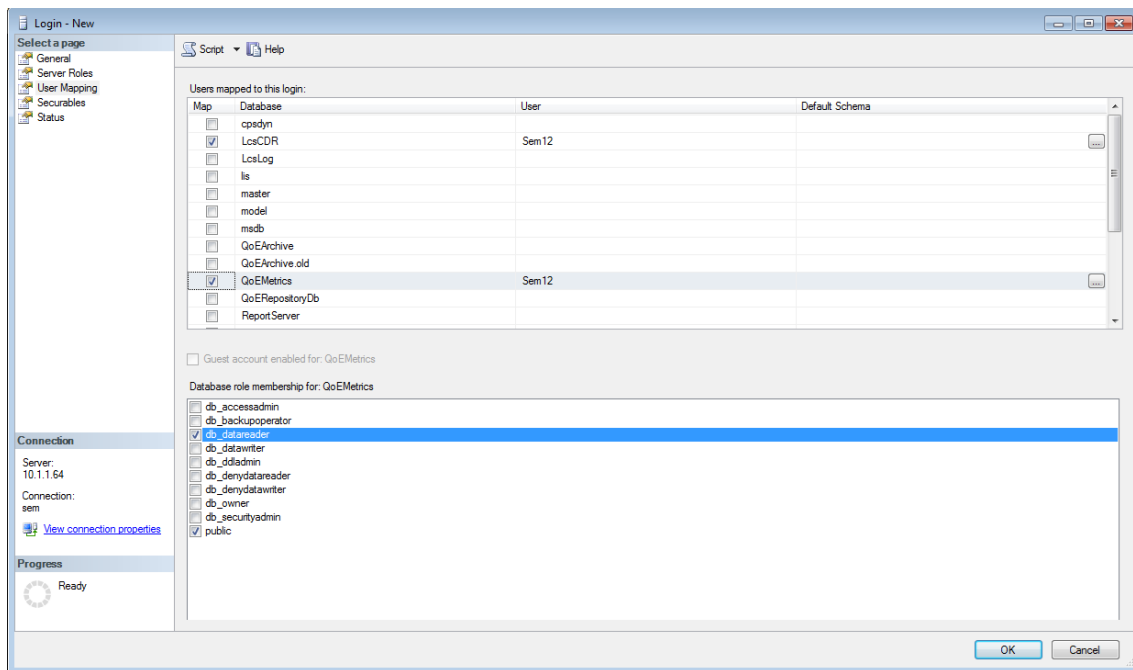
Connection: SA

[View connection properties](#)

4. Under 'User Mapping' shown in the following figure, in the 'Users mapped to this login' pane, select **LcsCDR** and in the 'Database role membership for LcsCDR' pane, select **db\_datareader** and **public**.

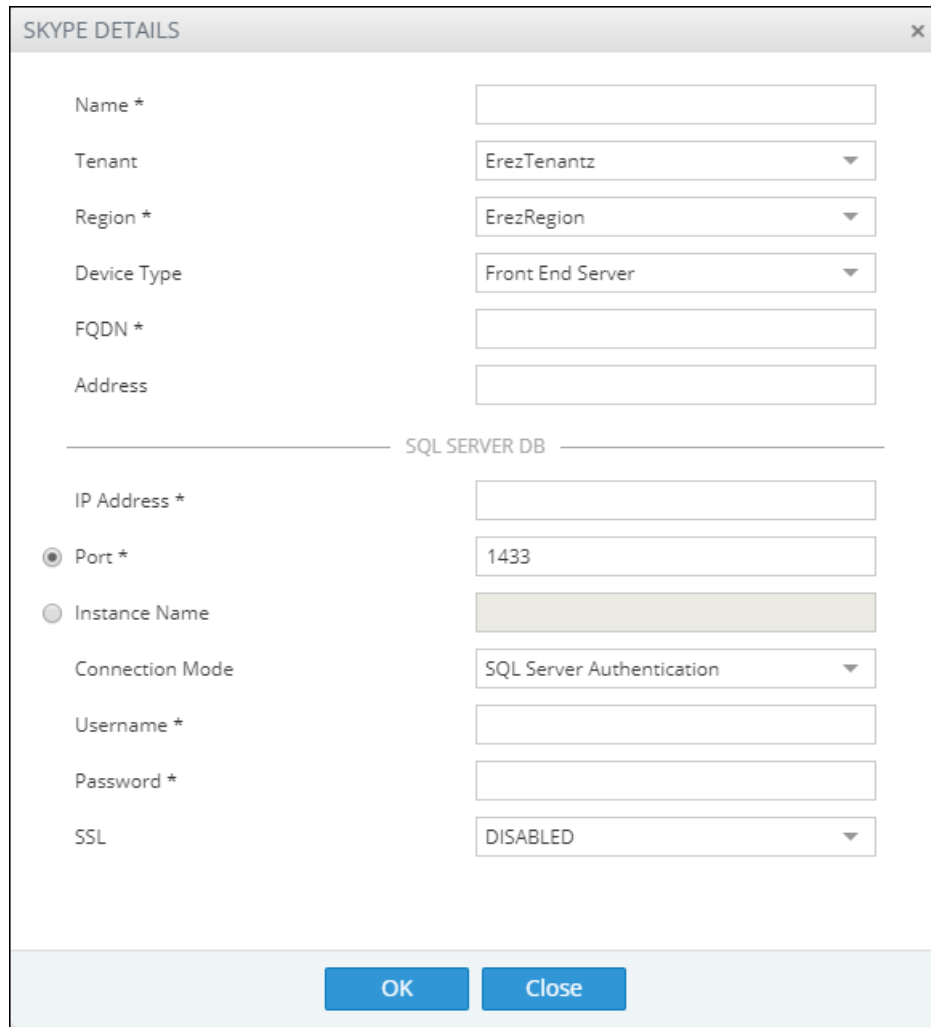
**Figure 12-4: Login Properties – User Mapping – db\_datareader | public**

- Under 'User Mapping' shown in the following figure, in the 'Users mapped to this login' pane, select **QoEMetrics** and then in the 'Database role membership for QoEMetrics' pane, select **db\_datareader** and **public**.

**Figure 12-5: User Mapping – QoEMetrics - db\_datareader | public**

The SQL server side is now ready.

- In the OVOC, under 'Network', click **Add** and then select **Skype Device**.

**Figure 12-6: Skype Details**

The image shows a 'SKYPE DETAILS' dialog box with a close button (X) in the top right corner. The dialog is divided into two sections by a horizontal line. The top section contains fields for 'Name \*', 'Tenant' (a dropdown menu showing 'ErezTenantz'), 'Region \*' (a dropdown menu showing 'ErezRegion'), 'Device Type' (a dropdown menu showing 'Front End Server'), 'FQDN \*', and 'Address'. The bottom section is titled 'SQL SERVER DB' and contains fields for 'IP Address \*', 'Port \*' (with a radio button selected), 'Instance Name' (with a radio button), 'Connection Mode' (a dropdown menu showing 'SQL Server Authentication'), 'Username \*', 'Password \*', and 'SSL' (a dropdown menu showing 'DISABLED'). At the bottom of the dialog are two buttons: 'OK' and 'Close'.

SKYPE DETAILS	
Name *	<input type="text"/>
Tenant	<input type="text" value="ErezTenantz"/>
Region *	<input type="text" value="ErezRegion"/>
Device Type	<input type="text" value="Front End Server"/>
FQDN *	<input type="text"/>
Address	<input type="text"/>
SQL SERVER DB	
IP Address *	<input type="text"/>
<input checked="" type="radio"/> Port *	<input type="text" value="1433"/>
<input type="radio"/> Instance Name	<input type="text"/>
Connection Mode	<input type="text" value="SQL Server Authentication"/>
Username *	<input type="text"/>
Password *	<input type="text"/>
SSL	<input type="text" value="DISABLED"/>
<input type="button" value="OK"/> <input type="button" value="Close"/>	

7. From the 'Device Type' drop-down, select **Front End Server**.
8. Enter the SQL Server IP address.
9. Select the **SQL Port** option and leave the default unchanged.
10. Click the 'Address' field, enter the first letter of the location, and from the list displayed, select it.
11. Enter the other details about your Microsoft SQL server - use the user credential defined previously in the SQL server.

**This page is intentionally left blank.**

**International Headquarters**

1 Hayarden Street,  
Airport City  
Lod 7019900, Israel  
Tel: +972-3-976-4000  
Fax: +972-3-976-4040

**AudioCodes Inc.**

200 Cottontail Lane  
Suite A101E  
Somerset NJ 08873  
Tel: +1-732-469-0880  
Fax: +1-732-469-2298

**Contact us:** <https://www.audiocodes.com/corporate/offices-worldwide>

**Website:** <https://www.audiocodes.com/>

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-91046

